This chapter takes you through the various policies laid to minimize cyber risk. It is only with well-defined policies that the threats generated in the cyberspace can be reduced.

**Promotion of R&D in Cybersecurity**

Due to the ever-increasing dependence on the Internet, the biggest challenge we face today is the security of information from miscreants. Therefore, it is essential to promote research and development in cybersecurity so that we can come up with robust solutions to mitigate cyber risks.

**Cybersecurity Research**

Cybersecurity Research is the area that is concerned with preparing solutions to deal with cyber criminals. With increasing amount of internet attacks, advanced persistent threats and phishing, lots of research and technological developments are required in the future.

**Cybersecurity Research-Indian Perspective**

In the recent years, India has witnessed an enormous growth in cyber technologies. Hence it calls for an investment in the research and development activities of cybersecurity. India has also seen many successful research outcomes that were translated into businesses, through the advent of local cybersecurity companies.

**Threat Intelligence**

Research work to mitigate cyber-threats is already being commenced in India. There is a proactive response mechanism in place to deal with cyber threats. Research and Development activities are already underway at various research organizations in India to fight threats in cyberspace.

**Next Generation Firewall**

Multi-identity based expertise such as Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

**Secured Protocol and Algorithms**

Research in protocols and algorithms is a significant phase for the consolidation of cybersecurity at a technical level. It defines the rules for information sharing and processing over cyberspace. In India, protocol and algorithm level research includes –

- Secure Routing Protocols
- Efficient Authentication Protocols
- Enhanced Routing Protocol for Wireless Networks
- Secure Transmission Control Protocol
- Attack Simulation Algorithm, etc.

**Authentication Techniques**

Authentication techniques such as Key Management, Two Factor Authentication, and Automated key Management provide the ability to encrypt and decrypt without a centralized key management system and file protection. There is continuous research happening to strengthen these authentication techniques.

**BYOD, Cloud and Mobile Security**
With the adoption of varied types of mobile devices, the research on the security and privacy related tasks on mobile devices has increased. Mobile security testing, Cloud Security, and BYOD BringYourOwnDevice risk mitigation are some of the areas where a lot of research is being done.

**Cyber Forensics**

Cyber Forensics is the application of analysis techniques to collect and recover data from a system or a digital storage media. Some of the specific areas where research is being done in India are –

- Disk Forensics
- Network Forensics
- Mobile Device Forensics
- Memory Forensics
- Multimedia Forensics
- Internet Forensics

**Reducing Supply Chain Risks**

Formally, supply chain risk can be defined as –

> Any risk that an opponent may damage, write some malicious function to it, deconstruct the design, installation, procedure, or maintenance of a supply item or a system so that the entire function can be degraded.

**Supply Chain Issues**

Supply chain is a global issue and there is a requirement to find out the interdependencies among the customers and suppliers. In today’s scenario it is important to know – What are the SCRM problems? and How to address the problems?

An effective SCRM SupplyChainRiskManagement approach requires a strong public-private partnership. Government should have strong authorities to handle supply chain issues. Even private sectors can play a key role in a number of areas.

We cannot provide a one-size-fits-all resolution for managing supply chain risks. Depending on the product and the sector, the costs for reducing risks will weigh differently. Public Private Partnerships should be encouraged to resolve risks associated with supply chain management.

**Mitigate Risks through Human Resource Development**

Cybersecurity policies of an organization can be effective, provided all its employees understand their value and exhibit a strong commitment towards implementing them. Human resource directors can play a key role in keeping organizations safe in cyberspace by applying the following few points.

**Taking Ownership of the Security Risk Posed by Employees**

As most of the employees do not take the risk factor seriously, hackers find it easy to target organizations. In this regard, HR plays a key role in educating employees about the impact their attitudes and behavior have on the organization's security.

**Ensuring that Security Measures are Practical and Ethical**

Policies of a company must be in sync with the way employees think and behave. For example, saving passwords on systems is a threat, however continuous monitoring can prevent it. The HR team is best placed to advise whether policies are likely to work and whether they are appropriate.

**Identifying Employees who may Present a Particular Risk**
It also happens that cyber-criminals take the help of insiders in a company to hack their network. Therefore it is essential to identify employees who may present a particular risk and have stringent HR policies for them.

Creating Cybersecurity Awareness

Cybersecurity in India is still in its evolution stage. This is the best time to create awareness on issues related to cyber security. It would be easy to create awareness from the grass-root level like schools where users can be made aware how Internet works and what are its potential threats.

Every cyber café, home/personal computers, and office computers should be protected through firewalls. Users should be instructed through their service providers or gateways not to breach unauthorized networks. The threats should be described in bold and the impacts should be highlighted.

Subjects on cybersecurity awareness should be introduced in schools and colleges to make it an ongoing process.

The government must formulate strong laws to enforce cybersecurity and create sufficient awareness by broadcasting the same through television/radio/internet advertisements.

Information Sharing

United States proposed a law called Cybersecurity Information Sharing Act of 2014 CISA to improve cybersecurity in the country through enhanced sharing of information about cybersecurity threats. Such laws are required in every country to share threat information among citizens.

Cybersecurity Breaches Need a Mandatory Reporting Mechanism

The recent malware named Uroburos/Snake is an example of growing cyber-espionage and cyber-warfare. Stealing of sensitive information is the new trend. However, it is unfortunate that the telecom companies/internet service providers ISPs are not sharing information pertaining to cyber-attacks against their networks. As a result, a robust cybersecurity strategy to counter cyber-attacks cannot be formulated.

This problem can be addressed by formulating a good cybersecurity law that can establish a regulatory regime for obligatory cybersecurity breach notifications on the part of telecom companies/ISPs.

Infrastructures such as automated power grids, thermal plants, satellites, etc., are vulnerable to diverse forms of cyber-attacks and hence a breach notification program would alert the agencies to work on them.

Implementing a Cybersecurity Framework

Despite the fact that companies are spending on cybersecurity initiatives, data breaches continue to occur. According to The Wall Street Journal, “Global cybersecurity spending by critical infrastructure industries was expected to hit $46 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc.” This calls for the effective implementation of the cybersecurity framework.

Components of Cybersecurity Framework

The Framework comprises of three main components –

- The Core,
- Implementation Tiers, and
- Framework Profiles.
The Framework Core

The Framework Core is a set of cybersecurity activities and applicable references that having five simultaneous and constant functions — Identify, Protect, Detect, Respond, and Recover. The framework core has methods to ensure the following —

- Develop and implement procedures to protect the most critical intellectual property and assets.
- Have resources in place to identify any cybersecurity breach.
- Recover from a breach, if and when one occurs.

The Implementation Tiers

The Framework Implementation Tiers define the level of sophistication and consistency an organization employs in applying its cybersecurity practices. It has the following four levels.

**Tier 1 Partial** — In this level, the organization’s cyber-risk management profiles are not defined. There is a partial consciousness of the organization’s cybersecurity risk at the organization level. Organization-wide methodology to managing cybersecurity risk has not been recognized.

**Tier 2 RiskInformed** — In this level, organizations establish a cyber-risk management policy that is directly approved by the senior management. The senior management makes efforts to establish risk management objectives related to cybersecurity and implements them.

**Tier 3 Repeatable** — In this level, the organization runs with formal cybersecurity measures, which are regularly updated based on requirement. The organization recognizes its dependencies and partners. It also receives information from them, which helps in taking risk-based management decisions.

**Tier 4 Adaptive** — In this level, the organization adapts its cybersecurity practices "in real-time" derived from previous and current cybersecurity activities. Through a process of incessant development in combining advanced cybersecurity technologies, real-time collaboration with partners, and continuous monitoring of activities on their systems, the organization’s cybersecurity practices can quickly respond to sophisticated threats.

The Framework Profile

The Framework Profile is a tool that provides organizations a platform for storing information concerning their cybersecurity program. A profile allows organizations to clearly express the goals
of their cybersecurity program.

**Where do You Start with Implementing the Framework?**

The senior management including the directors should first get acquainted with the Framework. After which, the directors should have a detailed discussion with the management about the organization’s Implementation Tiers.

Educating the managers and staff on the Framework will ensure that everyone understands its importance. This is an important step towards the successful implementation of a vigorous cybersecurity program. The information about existing Framework Implementations may help organizations with their own approaches.