NURTURE
Education Solutions
TOMORROW'S HERE

Subject: Cybersecurity Fundamentals

Module Number: 05

Module Name: Cybersecurity Framework - Indian Context

Syllabus

Cybersecurity Framework – Indian Context

Understanding National Cybersecurity Policy, DSCI (Data Security Council of India) Security Framework, Data Privacy Attacks, Data linking and profiling, Privacy on the Web, Email Security, Privacy Impacts of Emerging Technologies, Overview of RBI Guidelines on Cybersecurity Framework, case study on latest data breaches in India and lessons learnt

Cybersecurity Framework-Indian Context

Aim:

This module aims to equip students with fundamentals and characteristics of Cybersecurity.

Objectives:

The objectives of this module are to:

- Define Cybersecurity.
- Elaborate the Framework of Cybersecurity.
- List out and understand the National Cybersecurity Policy.
- Interpret the DSCI Framework.
- Formulate the RBI guidelines on Cybersecurity Framework.
- Examine the case study on latest data breaches in India and lessons learnt.

Outcomes:

At the end of this module, students are expected to:

- Define the concepts of Cybersecurity.
- Elaborate the Framework of Cybersecurity.
- State National Cybersecurity Policy.
- Sketch the DSCI Framework.
- Interpret the RBI guidelines on Cybersecurity Framework.
- Analyze a case study on the latest data breaches in India and lessons learnt.

Table of Contents

Understanding National Cybersecurity Policy

- Nationwide Cybersecurity Policy is a policy framework by the Department of Electronics and Information Technology.
- Its aim is to keep public and private infrastructure safe from cyber-attacks. "Information, such as personal information (of site users), financial and banking information, and sovereign data," according to the policy.
- National Cybersecurity policy - “For secure computing environment and adequate trust and confidence in electronic transactions ”

Why the Policy Required?

- To prevent cyber-attacks on the country's critical information infrastructures.
- To reduce national vulnerability to cyber-attacks.
- To minimise cyber-attack damage and recovery time.
- To establish a technical-professional body that certifies network security to ensure the overall health of government systems.

Why Cybersecurity has become essential now?

- Mischievous acts in cyberspace have evolved from inexperienced hackers to organised criminal gangs that are going Hi-tech
- Increasing threat to national security – web espionage evolves from a curiosity to well-funded and well-organised operations aimed at a financial and political or technical gain.
- Increasing threat to online services – individuals and industry are affected as attack techniques become more sophisticated.
- Internet has become a weapon for political, military and economic espionage
- Organised cyber-attacks have been witnessed in the last few years:
- Pentagon, US in 2007
- Estonia in April 2007

Why Cybersecurity has become essential now? (Contd….)

- Computer systems of German Chancellery and three Ministries
- E-mail accounts at National Informatics Centre, India
- Highly classified Govt. computer networks in New Zealand and Australia
- The software used to carry out these attacks indicate that they were clearly designed and tested with much greater resources than usual individual hackers
- Online services are becoming prime targets for cybercriminals
- Cyber offenders continue to refine their means of deceit as well as their victims. In summary, the global threats affecting users in 2008 are:
- New and sophisticated forms of attacks

Why Cybersecurity has become essential now? (Contd….)

- Spams targeting new technologies, such as VoIP (vishing – phishing via VoIP and phreaking – hacking tel networks to make free long-distance calls) and peer-to-peer services
- Attacks targeting online social networks
- Assaults targeting online services, particularly online banking services

Who is Responsible for ensuring Virtual Space free of Cyber Threat?

- Government
- Private sector
- Users
- Academicians

Actions needed to be taken at different levels

At County Level:

- Compliance, liability and enforcement of policy directives on data security and privacy protection (ex. Information Technology Act 2000).
- Compliance standards and guidelines (ex: ISO 27001, ISO 20001 and CERT-In guidelines).
- Infrastructure for conformity assessment (allowing and endorsing actions related to security products – ISO 15408, security processes – ISO 27001, and security manpower – CISA, CISSP, ISMS-LA, DISA and so on).
- Early notice and response to a security incident (National cyber alert system and crisis management).

Actions needed to be taken at different levels

At Corporate Level:

- Security best practices (e.g. ISO27001), service quality (ISO 20001) and service-level agreements (SLAs) compliance and demonstration
- Net traffic monitoring, routing and gateway controls are used to take proactive measures to deal with and contain harmful activities and ensure service quality and safeguard typical end-users.
- To stay current, keep up with developments in security technology and processes (configuration, patch and vulnerability management)
- Personnel involved in security-related tasks should be trained and updated regularly.
- For the sake of safe computing both inside and outside, encourage responsible user behaviour.

Actions needed to be taken at different levels

Small User Level:

- Maintain the level of alertness required for self-defence.
- Use legal software and update it on a regular basis.
- When using the internet, be aware of security risks and follow any security cautions that may be issued.
- To avoid misuse of computer resources, maintain a reasonable and trustworthy access control system.

How this policy can check cyber crime?

By facilitating international cooperation arrangements:

- Governments are expected to become more aggressive in the coming years, pursuing action against specific individuals/groups/companies, regardless of location.
- Governments are also likely to start placing pressure on intermediary organisations with the skills and resources to safeguard the public from malware, hacking and social engineering, such as banks, ISPs and software vendors.
- We might see industry-specific norms of practice requiring enhanced security procedures, backed up by assurance and insurance programmes.

How this policy can check cyber crime? (Contd….)

By facilitating international cooperation arrangements:

- **Enabling the government, as a key stakeholder**, to provide an adequate environment/conditions for data security and privacy protection concerns through policies and legal/regulatory framework. The National Cybersecurity Policy would ensure that the Indian IT Act is amended, and that a security and privacy assurance framework and crisis management plan (CMP) are designed.
- **Providing user agencies in the government and key sectors** with the tools they need to strengthen the security posture of their IT systems and networks and their ability to resist cyber-attacks and recover in a reasonable time if they do occur.
- Increase public understanding of cybersecurity and communicate government policies on cybersecurity through **public communication and outreach campaigns.**

Security Assurance Ladder

The importance of security control is determined by the type of environment.

Low risk: 'Awareness' — be aware of your security risks and adhere to industry best practices.

Medium risk: ‘Awareness and Action' — Proactive techniques help you deal with security threats and incidents more effectively.

High risk: ‘Awareness, Action, and Assurance' - Because security failures can be disastrous and result in unaffordable repercussions, assurance (a basis of trust and confidence) is needed that security controls work when they are needed is critical.

Cybersecurity Framework-Indian Context

Strategies

- Creating a secured ecosystem.
- Creating an assurance framework.
- Encouraging open standards.
- Strengthening the regulatory framework.
- Creating a mechanism for security threats early warning, vulnerability management and response to a security threat.
- Securing e-governance services.
- Protection and resilience of critical information infrastructure.
- Promotion of research and development in cybersecurity and reducing supply chain risks.

DSCI Security Framework

- In cyberspace, the concept of privacy has expanded significantly from its traditional meaning of intrusion into one's physical environment. Consumer data privacy is becoming a basic right.
- It is recognised as a fundamental right in several countries, protected by the constitution and accompanying legal framework.
- Numerous countries share the goal of improving citizen privacy protection. In general, each country has a different approach to privacy.
- DSCI has conceptualised it’s approach to privacy in the DSCI Privacy Framework, which is based on global privacy best practices and frameworks, to protect the privacy of personal information against unauthorised use, disclosure, alteration or exploitation.

DSCI Security Framework (Contd….)

Three layers of the DSCI framework:

Privacy Strategy and Processes: This layer supports the development of privacy's strategic and tactical elements. It is creating visibility into personal data aids in understanding how an organisation handles data. The central privacy organisation should track personal information processed by an organisation's procedures, functions, projects, and activities. It should form strong bonds with various parts of an organisation to coordinate and collaborate on privacy issues. The privacy policy should serve as a roadmap for implementing privacy, and it should be backed up by systems that guarantee consistency in the effectiveness of privacy protections.

DSCI Security Framework

Three layers of the DSCI framework

Information Usage, Access, Monitoring and Training: This layer guarantees that an organisation has a sufficient level of awareness. To limit information usage and access, a number of safeguards have been implemented. In addition, a method for privacy monitoring and incident management has been implemented.

Personal Information Security: The security initiatives of an organisation provide strength to this layer. It does, however, necessitate an emphasis on data security. The DSCI has created a Protection Framework that can be used to ensure the security of personal data.

DSCI Security Framework

Approach to the Security Discipline: DSCI believes that examining the approaches, trends and practices that are driving a particular discipline is critical. The DSCI approach to the subject under consideration is articulated in this section of each discipline.

Strategy for the Security Discipline: DSCI further believes that each security discipline merits a strategic treatment that will mature its effort and maximize the resources and efforts committed. DSCI recommends methodologies and processes for each discipline that aid in conducting a strategic assessment of an organization's endeavour. This section assists managers in giving the organisation's endeavours in each discipline a strategic direction.

DSCI Security Framework (Contd….)

Best Practices for the Security Discipline: DSCI recognises the need for thorough guidance on planning and implementing security in an organisation in an organised manner. This section of the DSF compiles with the best practices for the security implemented under each discipline.

The maturity of the Security Discipline: DSCI believes that assessing outcomes is important, and that understanding proper limits is required for a fair assessment. The maturity standards for each discipline are defined in this section by the DSF.

DSCI Security Framework (Contd….)

Best Practices of DSF Include:

- Security Strategy and Policy
- Asset Management (ASM)
- Governance Risk and Compliance (GRC)
- Infrastructure Security (INS)
- Application Security (APS)
- Secure Content Management (SCM)
- Threat and Vulnerability Management (TVM)
- User Access and Privilege Management (UAP)
- Business Continuity and Disaster Recovery Management (BDM)

Data Privacy

Data privacy, also known as information privacy, is a subset of data protection that deals with the proper handling of sensitive data, most particularly personal data, but also other confidential data, such as certain financial data and intellectual property data, in order to comply with regulatory requirements while maintaining the data's confidentiality and immutability.

Personal data breaches can comprise:

- Access by an unauthorised third party,
- Deliberate or unintentional action (or inaction) by a controller or processor,
- Sending personal data to the wrong recipient,
- Computing devices containing personal data being lost or stolen,
- Alteration of personal data without permission, and loss of availability of personal data.

Data Privacy (Contd….)

Data Privacy Attacks:

Phishing: These social engineering attacks are intended to deceive you into allowing a data breach to occur. To easily deceive you, phishing attackers appear as people or organisations you trust. Criminals of this type try to persuade you to give up access to sensitive information or to provide the information itself.

Brute Force Attacks: Hackers may use software tools to guess your credentials in a more brazen method.

Malware: Security holes can exist in our device's operating system, software, hardware or the network and servers to which you are connected. Criminals look for these security flaws because they are ideal places to hide malware. Spyware, in particular, is great for obtaining personal information while remaining unnoticed. It is possible that you won't notice this infection until it is too late.

Data Profiling

- The process of evaluating, analysing and developing relevant summaries of data is known as data profiling. The procedure generates a high-level overview that aids in the identification of data quality concerns, risks and overall trends.
- Data profiling provides key data insights that businesses can use to their advantage.
- Data profiling can help you to avoid costly mistakes in your client database. These errors include missing values, values that should not be included, values with unusually high or low frequency, values that do not follow expected patterns and values outside the normal range.

Data Profiling

Benefits of Data Profiling:

- **Better data quality and credibility**: After the data have been evaluated, the application can assist in the removal of duplicates or abnormalities. It can be used to discover important information that could influence business decisions, uncover quality issues inside an organisation's system and draw specific inferences about a company's future health.
- **Predictive decision making**: Profiled data can be used to prevent minor errors from becoming major issues. It can also reveal what might happen in new settings. Data profiling aids in the creation of an accurate picture of a company's health in order to better guide decision-making.

Data Profiling

Benefits of Data Profiling:

- **Proactive crisis management**: Data profiling can assist in identifying and resolving issues fast, often before they develop.
- **Organized sorting**: Most databases work with a wide range of data, including blogs, social media and other big data markets. Profiling can track data back to its source and ensure that it is properly encrypted for security. After then, a data profiler can examine those databases, source apps or tables to ensure that the data meet normal statistical metrics and business regulations.

Privacy on the Web

- The right to privacy on the Internet, also known as online privacy, is a subset of data privacy and a fundamental human right.
- It basically relates to your right to personal privacy when you show, store or provide information about yourself on the Internet.
- This can comprise both personally identifiable information (PII) and non-personally identifiable information (NPI), such as your online conduct.
- All of your online activities are being collected and analysed by interested parties if you don't use Internet privacy.

Privacy on the Web (Contd….)

Protect Privacy and Security on the Internet

- Secure your web Browser
- Use VPN
- Keep your software up-to-date
- Install an Antivirus program and activate firewall
- Delete cookies at browser exit
- Use HTTPs to secure
- Secure end-to-end encryption
- Share online files securely password protected

E-mail Security

- E-mail security refers to the methods and strategies used to safeguard email accounts, information and communication from unwanted access, loss or compromise.
- Malware, spam and phishing assaults are frequently disseminated over email.
- Attackers employ false messages to persuade users to divulge personal information, open attachments, or click on hyperlinks that download malware to the victim's device.
- Attackers attempting to get a foothold in an enterprise network and obtain valuable company data frequently use email as an entry point.
- Email encryption encrypts or disguises the content of emails to prevent sensitive information from being read by anybody other than the intended receivers. Authentication is frequently included in email encryption.

E-mail Security

Security Features:

- Spam Filters
- Anti-virus Protection
- Image and Content Control
- Data Encryption

Overview of RBI guidelines on Cybersecurity Framework

- The RBI Cybersecurity Framework Guidelines will allow banks to formalise and implement a Cybersecurity strategy and a cyber crisis management plan. The need for Cybersecurity incidents to be reported to RBI would also aid in the structure of proactive threat identification and mitigation.
- RBI defined proper guidelines on measures of cybersecurity approach, a recent survey conducted by https.in Of the top 10 PSU Bank SSL certificate, is evident that the RBI guidelines are followed.
- Cybersecurity operations centre (SOC): RBI understands the need for a secured ecosystem that can ensure proactive information sharing and a flexible framework. Therefore, RBI guidelines clearly state the need for setting up a cybersecurity operations centre. As per guidelines, a focus on a secured ecosystem from top management and cyber-aware board is expected.

Overview of RBI guidelines on Cybersecurity Framework (Contd….)

RBI Guidelines:

- **Securing client data and its usage in financial crimes**: RBI has a very clear and strong emphasis on the data security of customers.
- The banks are required to adopt the highest possible preventive measures to secure customer's data whether it is in motion or freeze state. Guidelines further focus on organising such programmes where customers can make aware of reducing the incidents of attacks.
- **Proactive reporting and collaboration**: RBI has recognised the importance of collaboration between different financial institutions, which would help them mutually and make them capable of responding to the attacks proactively and quickly.

Overview of RBI guidelines on Cybersecurity Framework (Contd….)

RBI Guidelines:

- **Infinite surveillance**: A much important, continuous surveillance and real-time analysis was required as it helps in taking actions faster when attacked from outside. New guidelines would require banks to implement 24*7 real-time-based surveillance.
- These measures not only reduce the impact of loss but also help in deciding an effective measure to stop such incidences in the future.
- **Cyber Crisis Management Plan (CCMP):** The RBI circular calls for the establishment of a Cyber Crisis Management Plan to address the full lifecycle of detection, response, containment and recovery.

Case Study On Latest Data Breaches In India And Lessons Learnt

- May 2021 – The Air-India data breach of more than 4.5 million passengers after a sophisticated cyber-attack on SITA – the Switzerland-based company providing passenger services system. The attack was carried out on its servers based in the US.
- March 2021 – Ransomware attack on Pimpri-Chinchwad Municipal Corporation, Smart City project in Pune district, managed by Tech Mahindra.
- In October 2020 – Haldiram's popular food major faced the ransomware attack, and attackers demanded $7,50,000 for access.
- November 2020 – The Indian Computer Emergency Response Team (CERT-In) issued a warning against the spread of ransomware virus 'Egregor' capable of stealing vital corporate data.

Case Study On Latest Data Breaches In India And Lessons Learnt

- Attacks on India's CoWIN app
- The Black Kingdom ransomware targets Microsoft Exchange servers
- LinkedIn phishing scam

Summary

- The framework is intended to be sufficiently adaptable to be utilised by associations with developing digital security and risk administration programs and those with less-created programs.
- The Cybersecurity Framework is for associations of all sizes, divisions, and developments. The framework was designed to be extremely adaptable. With a built-in customisation option available, the framework can be modified to be used by any organisation.
- A framework profile ('Profile') represents the outcomes based on business needs that an organisation has selected from the Framework Categories and Subcategories.
- An organisation can use the framework as a critical part of its systematic process for identifying, assessing and managing cybersecurity risk.

Self Assessment Question

1. PCI DSS stands for _____.

a. Payment Card Industry Data Security Standard

b. Payment Card Information Data Security Standard

c. Both a and b

d. None of the above

Answer: a

Self Assessment Question

2. Which of the following is a core function of Cybersecurity framework?

a. Identify

b. Protect

c. Detect

d. All of the above

Answer: d

Self Assessment Question

3. CCMP stands for _____.

a. Cyber Crisis Management Plan

b. Cyber Crime Management Plan

c. Cyber Critical Management Plan

d. None of the above

Answer: a

Self Assessment Question

4. NHS stands for _____.

a. National Health Service

b. National Health Software

c. Network Health Service

d. None of the above

Answer: a

Self Assessment Question

5. DSCI stands for _____.

a. Data Security Community of India

b. Digital Security Council of India

c. Data Security Council of India

d. None of the above

Answer: c

Assignment

1. What is Cybersecurity?
2. Explain the core functions of Cybersecurity.
3. Explain DSCI.
4. List the guidelines from RBI regarding Cybersecurity.
5. List and explain core functions of Cybersecurity framework.

Document Link

Topic	URL
Cybersecurity	https://digitalguardian.com/blog/what-cyber-security
Cybersecurity Framework	https://www.edureka.co/blog/cybersecurity-framework/
RBI Guidelines	https://www.https.in/blog/rbi-guidelines-cyber-security/
Internet Privacy	https://blog.reputationx.com/internet-privacy-definition
E-Mail Security	https://www.duocircle.com/content/email-security-services/types-of-email-security
Security Breaches	https://analyticsindiamag.com/ransomware-everywhere-dire-state-of-cybersecurity-in-2021/

Video Link

Topic	URL
Cybersecurity Framework	https://www.youtube.com/watch?v=J9ToNuwmyF0

E- Book Link

Topic	URL
Cyber Space	https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
National Cybersecurity	http://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf