Cyber Security Framework
(Fundamental principles for protecting IT Asset.)

[5]*Ajit Saha,*
Scientist-F, National Informatics Centre, A-Block, CGO-Complex,
Lodhi Road, New Delhi-110003

Abstract: The Cyber Security framework is a flexible architecture in accordance with state-mandated, industry specific and cyber security regulation. The Cyber Security Framework is consisted of five functions for risk assessment and risk treatment of an information security management System. These five functions are Identify, Protect, Detect, Response and Recover. These functions are high level abstraction of information security risk assessment and risk treatment. Identify, Protect and Detect are the part of Risk Assessment. These five functions were selected because they represent the five pillars of successful and holistic cyber security program. These functions act as the backbone of the framework.

This framework encompasses information security, IT infrastructure security, privacy protection and information security management system including electronic record retention schedule which manages and reduces the risk of information damage and any kind of cyber incidents. This framework can be used for determining and implementing controls for information security risk treatment in an information security management system. The cyber security framework is a layered architecture depicted in fig-1. for providing better management and protection to information security system of an organization. The advantage of layered architecture is very flexible and easily expandable also to manage the layer of security system with specific team of professionals, This framework is a coherent security management system with a holistic and coordinated approach in order to determine and implement security controls.

Swanirman Sunirmit
Explore Technology advancements for Sustainable Ecosystem or Society

Keywords : Cyber security framework, information security, cyber security, information security management

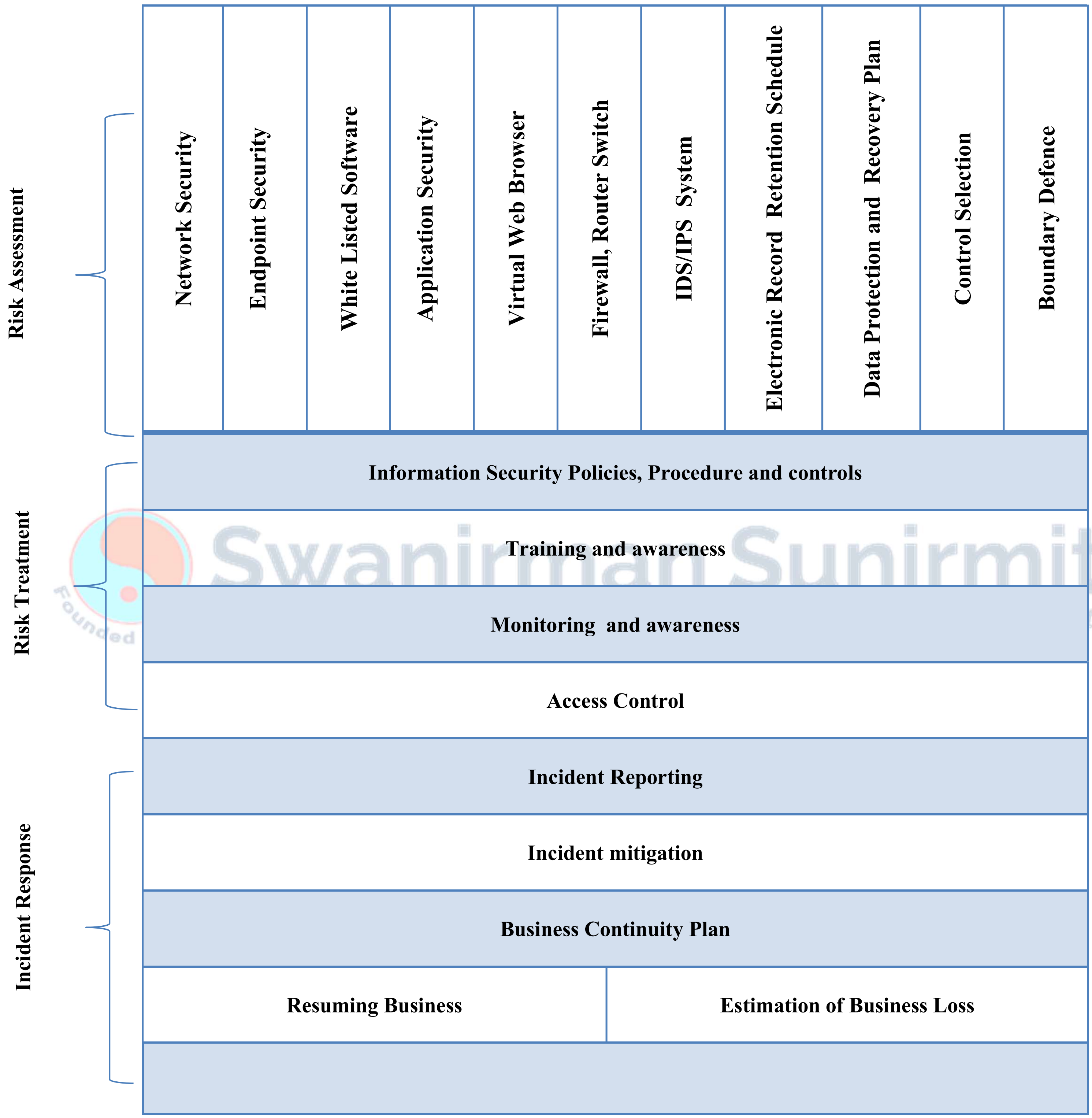
I. INTRODUCTION

The inevitability of risks is also part of the reason why all organizations must conduct **a risk assessment** and risk analysis. Since risk exists therefore the goal here is to identify the risk level so that the organization can implement multiple controls and interim measures to manage the impact of those risks on organization. The organization should set up IT infrastructure as per level of risk in the organization. It is not essential to implement all verticals in an organization. It depends on the Risk assessment.

The ***Risk treatmen****t* is a collection of terms for all the tactics , options and strategies and training chosen to respond to a specific risk to achieve the desired outcome concerning to the threat. Effective risk treatment is a continuous process that requires regular reassessment and adoption as new threats emerge and technology evolve.

A ***Business Mitigation Plan*** is a strategy or set of actions designed to reduce or manage risks that could negatively impact the operations, reputation, or financial stability of a business. This plan typically focuses on identifying potential threats to the business and implementing measures to either eliminate or reduce the likelihood and impact of those risks.

II. Cyber Security Framework diagram



Risk Assessment

Network Security

Endpoint Security

White Listed Software

Application Security

Virtual Web Browser

Firewall, Router Switch

IDS/IPS System

Electronic Record Retention Schedule

Data Protection and Recovery Plan

Control Selection

Boundary Defence

Risk Treatment

Information Security Policies, Procedure and controls

Training and awareness

Monitoring and awareness

Access Control

Incident Response

Incident Reporting

Incident mitigation

Business Continuity Plan

Resuming Business	Estimation of Business Loss

Swanirman Sunirmit

III. OUTCOME OF FRAMEWORK

The ***outcome of implementing a cybersecurity framework*** is the establishment of a robust, systematic approach to managing and mitigating cyber risks, thereby strengthening an organization's overall security posture. It provides a structured method for identifying, assessing, and reducing cyber threats while ensuring compliance with industry standards and regulations. It is important to recognize that cyber security is an ongoing process and organization must continually review and update their security measures to stay ahead of evolving threat. The outcome of the framework is an effective cyber security practices and ensures integrity, confidentiality, accessibility/availability, authenticity and non-repudiations of information.

Security Control is defined as a measure that modify or manage security risk in the cyber security framework. These controls can be divided into two categories, one is generic nature control, which can be defined in risk context and second one is controls other than generic nature control which are defined with respect to physical and technological environment.

IV. HOW TO DETERMINE INFORMATION SECURITY CONTROLS ?

Risk assessment of an organization is the key tool for determining information security controls. Risk assessment should include nation and international legislation and regulation. Risk assessment evolves from domain expert of the organization who are concerned with sensitivity of organization's information. Risk assessment will balance between resource deployment for implementing controls and potential business impact from security incident in the absence of controls. The result of a risk assessment should help guide and determine the appropriate management action for implementing controls necessary to protect against these risks.

For simplifying development of controls, are categories in four section.

(a) ***Technological controls :*** related with technology which are adopted in organization.
(b) ***Individual People control :*** Concern with individual people.
(c) ***Physical :*** Concern with physical object
(d) ***Organizational control :*** Other than above controls which are required for implementing security.

Each and every control is consisted of five attributes. These attributes are (i) Control Type (ii) Information Security properties (iii) Cyber Security Concepts (iv) Operational Capabilities (v) security domain

V. CONTROL TYPE

Control Type attribute defines when and how the control modifies the risk of security incident. The attribute values are

- ***Preventive :*** The control is intended to prevent the occurrence of an information security incident
- ***Detective :*** The control acts when an information security incident occurs.
- ***Corrective :*** The control acts after an information security incident occurs.

Therefore it can be concluded that Security control should be defined with due diligence with in the organization in consultation with domain expert taken into consideration of sensitivity of data. Security control is the heart of the cyber security framework.

REFERENCES

[1]. National Cybersecurity Reference Framework (NCRF)
Jan 30, 2024 · NCRF is a framework that sets the standard for cybersecurity in India. It focuses on critical sectors and provides guidelines to help organizations develop strong cybersecurity systems. The NCRF can serve as a template for critical sector entities to develop their own ...

[2]. Information on cyber laws and security - National Portal of India

[3]. Users can access information on cyber security strategy and research and development (R&D). ...

[4]. https://www.iasgyan.in/.../national-cybersecurity-reference-framewo...

Swanirman Sunirmit
Explore Technology advancements for Sustainable Ecosystem or Society
Founded in 2020

NATIONAL CYBERSECURITY REFERENCE FRAMEWORK - IAS Gyan
Jan 31, 2024 · Complementing the NCRF, three accompanying compendiums delve into global ...

[5]. Cyber Security in India - Springer
Mar 18, 2020 · This 'IITK Directions' book focuses on cyber security research, education & ...

[5]***Ajit Saha:*** The Author is a Scientist and interested in doing Research and Development. Interested area is exploring upcoming technology and identify security breaches of the technology to mitigate security risk. . The author has 30 years of long Research and Development experience for various government organizations. The author has long experience on Cyber Security and ethical hacking, works as a Deputy Chief Information Security office in various Ministry. The author has big contribution on design of Cyber Security Framework by following ISO/IEC/27001 family of standard. The author has long teaching experience, had taken part-time classes in various renown Institutions like IETE, JNU, Jamia Hamdard University etc. An author passionate about cyber security because of several key factors: 1.Personal Experience: They may have had a personal encounter with cyber threats, such as a data breach or a security incident, which made them realize the importance of protecting digital assets. This personal experience can create a deep, personal commitment to improving cybersecurity measures. 2.Growing Threat Landscape: The increasing prevalence of cyber threats and attacks in today's digital world can be a significant motivator. The complexity and scale of cyber threats—from identity theft to ransomware— highlight the critical need for robust security measures, fueling a passion to tackle these challenges. 3.Intellectual Challenge: Cyber security is a field filled with complex problems and constantly evolving technologies. For those with a keen interest in problem-solving and staying ahead of adversaries, the intellectual challenge and the need to continuously learn and adapt can be highly stimulating and fulfilling. 4.Protecting Privacy and Safety: A strong desire to protect individuals' privacy and safety online can drive passion. Authors in this field often aim to safeguard personal information and ensure that digital interactions are secure, which can be deeply satisfying and align with their values. 5.Impact and Relevance: Cyber security has a direct impact on almost every aspect of modern life, from personal finances to national security. The relevance of the field and its potential to make a significant difference in protecting people and organizations can be a powerful motivator. 6.Innovative Solutions: The field of cybersecurity is continually evolving, with new technologies and methods emerging to combat cyber threats. The opportunity to be at the forefront of innovation and to contribute to the development of cutting-edge solutions can be a major driving force.