Chapter 1
Fundamentals for Cyber Risk Management

S. Priya
http://orcid.org/0009-0003-3305-745X
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India

S. Thirumal
http://orcid.org/0000-0002-8497-8764
Vels Institute of Science, Technology, and Advanced Studies, India

S. P. Santhoshkumar
http://orcid.org/0000-0001-8531-759X
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India

S. Ramamoorthi
http://orcid.org/0000-0001-5152-278X
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India

M. Mohamed Sithik
http://orcid.org/0009-0005-3989-7198
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India

ABSTRACT

The importance of cyber risk management cannot be overstated in the digital era because the companies rely on technologies such as cloud computing, AI, IoT, and 5G which increases the attack surface and puts up against advanced threats. Fundamentals of Cyber Risk Management chapter discusses the main principles of

DOI: 10.4018/979-8-3693-8397-1.ch001

identifying, evaluating, and eliminating cyber risks and enhancing the resilience. It describes the risk lifecycle, including identification, assessment, treatment and monitoring and presents standards, including NIST CSF, ISO/IEC 27005, COBIT and FAIR. The challenges that are identified in the chapter are the measurement of risks, human factors, resource constraints of SMEs, and vulnerability of supply chains. It emphasizes the need to prevent, detect, respond and recover, and be in compliance with GDPR and CCPA. Lastly, it focuses on leadership, culture, and accountability in instilling cybersecurity into enterprise governance to develop adaptive, secure organizations.

1. INTRODUCTION

In the digital age, companies in all industries are becoming increasingly reliant on technology, interdependent systems, and process-driven, which are based on data. Whereas these innovations are highly beneficial in terms of efficiency and innovation, it is also creating a wide range of cyber threats to organizations. Cyber risk is a term used to describe the possibility of loss, disruption or damage due to cyber threats, including data breach, ransomware, phishing, insider abuse or critical infrastructure attack. Cyber risks are dynamic, borderless, and ever-changing unlike traditional risks, and they are due to the rapid change in technology, globalization and the increasing sophistication of the adversaries, since they are dynamic.

Cyber risk management can be defined as a methodical way of detecting, evaluating, reducing and tracking risks caused by cyber threats. Besides being a technical problem, it is also a strategic requirement that affects business continuity, compliance with regulations, consumer trust and national security.

1.1. Problem Statement

Contemporary cybersecurity risks are always transnational, often being both initiated and affected by multiple countries at the same time. The vulnerabilities to cyberattacks are regulatory gaps, haphazard legal frameworks, and the absence of coordinated international policies. Though each country is taking cybersecurity-related steps, effective prevention, detection, and response of cross-border cyber threats has not been achieved due to lack of effective global coordination of actions against such threats. Thus, the urgent necessity to develop coordinated international cooperation systems and alignment of policy frameworks to respond to changing global cyber threats is a pressing issue.