



Cybersecurity Strategy



t. NZ +64 9 570 2233 | t. VIC +61 3 9913 3248 | t. QLD +61 7 3194 3664 | t. NSW +61 2 9098 8206
www.kaonsecurity.co.nz | e. sales@kaonsecurity.co.nz | www.kaonsecurity.com.au | e. sales@kaonsecurity.com.au

Introduction

According to ISACA's annual State of Cybersecurity Survey report 2021, attacks have increased to a level not seen since 2018, this calls for a more concerted and broad-based approach to protecting critical information assets.

Cybersecurity threats are dynamic and insidious, organisations therefore need to be agile in evaluating and modifying their cybersecurity priorities based on a sound risk management approach that factors in the latest intelligence and real-world incidents, and is informed by enterprise-wide lessons learned.

Understanding the capability of cybersecurity within an enterprise means comprehensively analysing the operational efficiency and effectiveness of actions taken; resiliency of the people, processes, or technology in use; maturity of practices; gap analyses; total cost of ownership; and more, and doing it across the axis of risk.

While developing the cybersecurity strategy, organisations must consider standards, best practices, key performance indicators (KPI) and business goals.

A well-developed viable cybersecurity strategy, based on sound risk management practices, is critical to the defence of an organisation's assets. The strategy and associated implementation plan identifies the steps necessary to ensure that resources are allocated across the organisation as effectively as possible. It is a crucial roadmap that translates these priorities into actions in order to protect the organisation's most valuable assets.

Kaon Security assist organisations to build the foundation to a resilient and cyber-minded culture that is aimed at reducing risk. We work with organisations to develop a cybersecurity strategy that is realistic, achievable and tailored to suit their unique operational realities.

Why Create A Cybersecurity Strategy?

A cybersecurity strategy:

- Provides a proactive approach to risk
- Helps senior management prioritise investments to protect valuable information assets
- Provides visibility of the Information Technology environment
- Builds resilience in IT operations
- Reduces information security risk
- Promotes continuous improvement

Organisations Have Unique Requirements

Cybersecurity has few, if any, one-size-fits-all solutions. Each organisation is unique, as are its needs and goals. Although risks impact every enterprise, the ways in which they are affected are different, as is in the way in which they develop and deliver their cybersecurity strategy.

Cybersecurity Strategy can be developed as a high level document with or without detailed information stated in an implementation plan. Both approaches address the specific needs of the organisation (refer [Cybersecurity Strategy](#) diagram)

High Level Cybersecurity Strategy

Generally, a high level cybersecurity strategy covers the following areas:

- Strategy goals
- Scope definition
- Cybersecurity needs and objectives
- Key performance indicators
- Identify stakeholders
- Communication plan
- Implementation strategy

Detailed Cybersecurity Strategy

Detailed cybersecurity strategy typically consists of the topics in the high level cybersecurity strategy with lower-level details such as major tasks and activities. These major tasks and activities are aligned to the objectives and cover the following areas:

- Mission
- Vision
- Strategy goals (overarching and accompanying goals)
- Guiding principles
- Objectives as aligned to the goals
- Aligned to a cybersecurity framework e.g. (NIST CSF)
- Major tasks derived from each of the objectives
- Activities to meet the tasks
- Mapping the objectives to the tasks and the framework function
- Detailed cybersecurity implementation plan and schedule

Cybersecurity Strategy

The diagram below indicates the different layers pertaining to a High level and Detailed Cybersecurity Strategy

