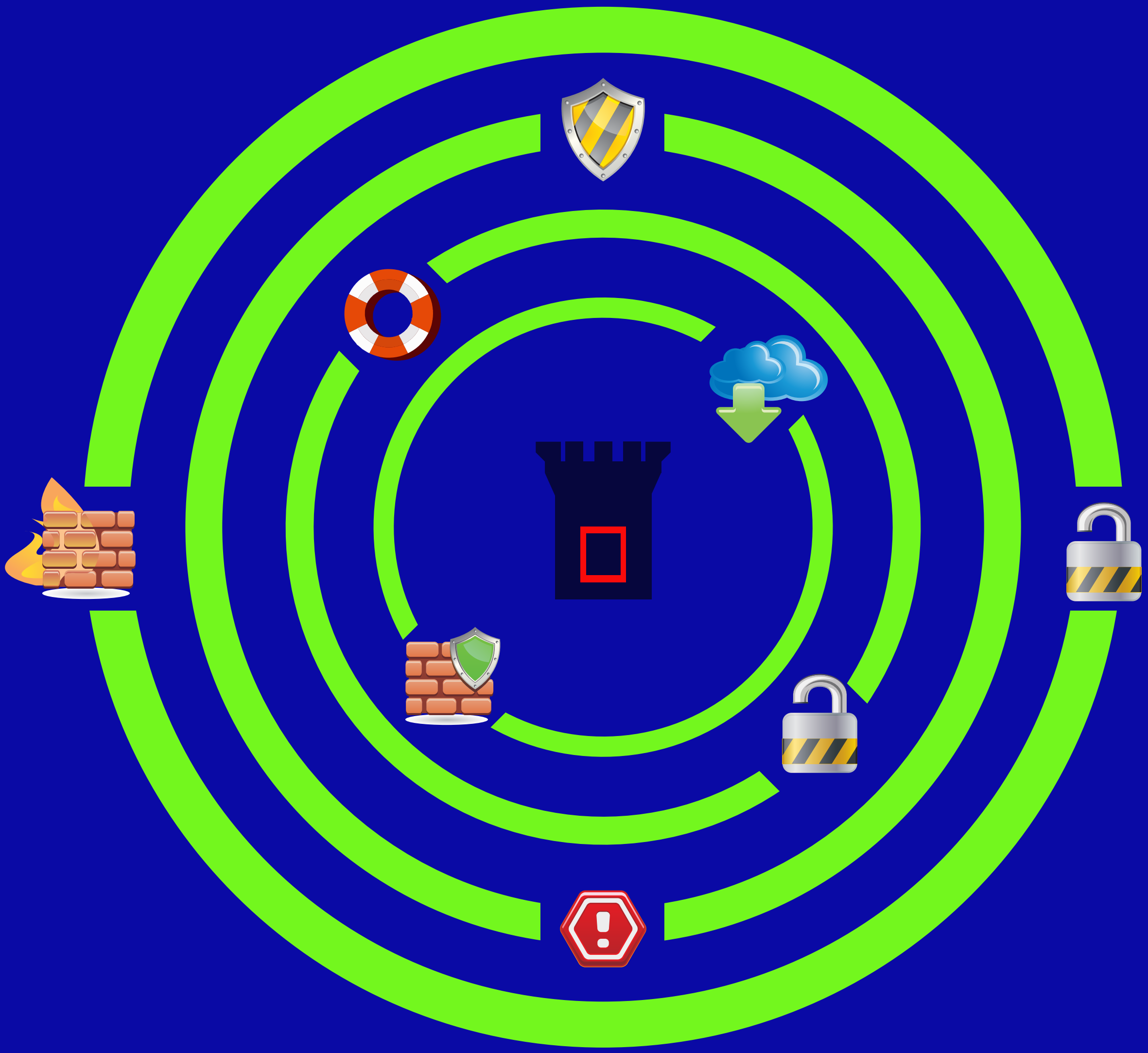
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Developing a Security Strategy



Happiest People . Happiest Customers

Contents

© Happiest Minds Technologies. All Rights Reserved

Introduction

What is a security strategy?

Business organizations develop and maintain strategic plans for most of the activities they carry out. Strategic plans define the need for an action, the impact of that particular action and driving forces behind the action. Security strategy in any organization starts with an in-depth analysis of their business. A security strategy is thus an important document which details out series of steps necessary for an organization to identify, remediate and manage risks while staying complaint. An effective security strategy is comprehensive and dynamic, with the elasticity to respond to any type of security threat. Developing a security strategy is a detailed process that involves initial assessment, planning, implementation and constant monitoring. It may also include a combination of actions that counter imaginable threats and vulnerabilities: policies and procedures, access management measures, communications systems, technologies and systems integration practices.

The security strategy document defines and prioritizes information assurance and security initiatives that the organization must commence to enhance the protection of information and related technology. Ideally an organization should consolidate previously identified and executed projects (where practical), provide scope and definition for each of the identified efforts, detail the general risks addressed by the initiative and provide a foundation that can later be refined by senior management. Additionally, to support higher-level evaluation of initiatives that can be undertaken when required, the security strategy planning process needs to identify any significant dependencies associated with the initiative

Strategy, planning and development

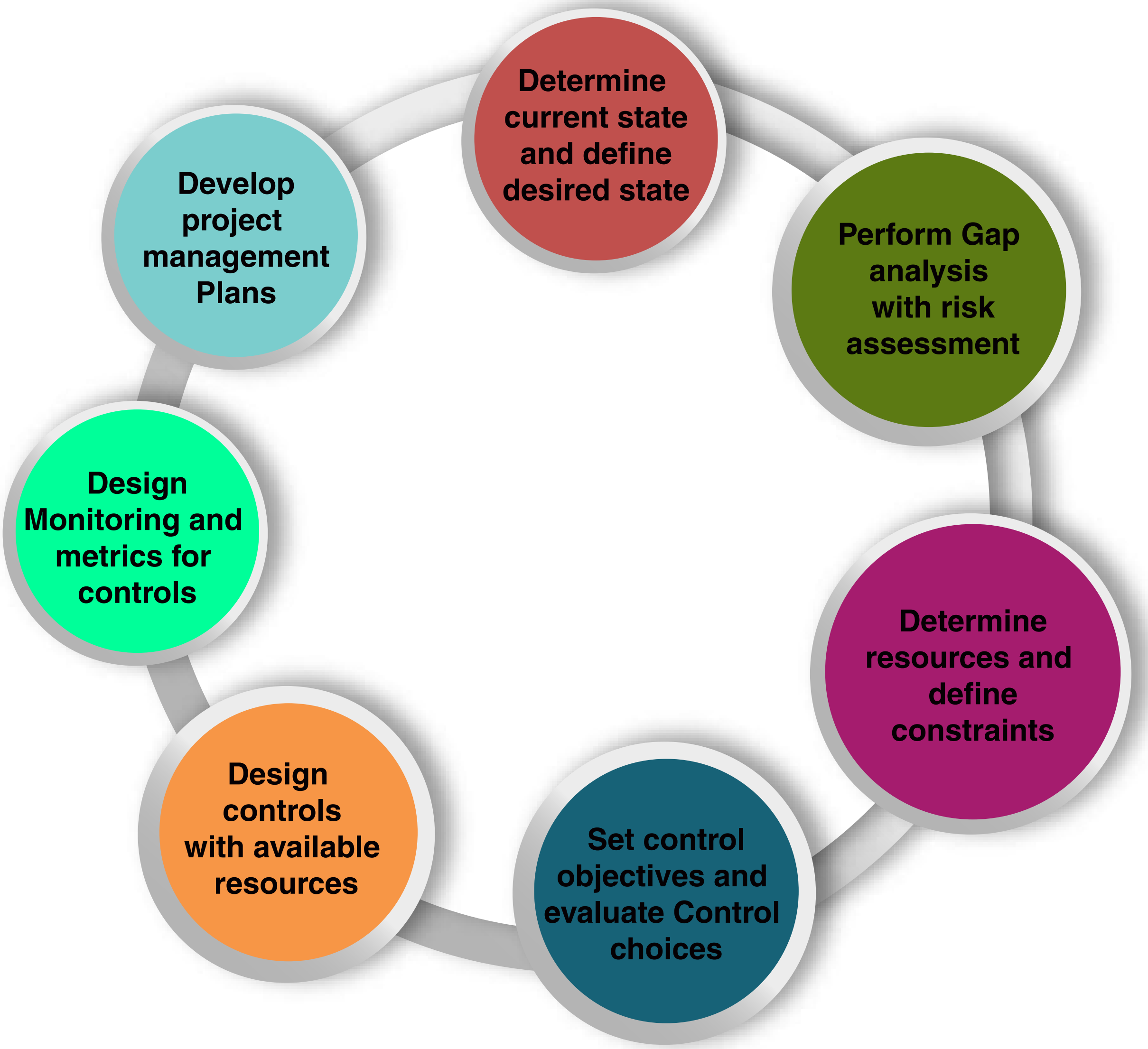
Leadership and management commitment

To protect an organization effectively through a well-planned security strategy, I.T, the important mission enabler, needs recognition as an important component of the organization. Effective and efficient information security programs require co –operation from business leaders and personnel within the organization along with clear direction and commitment from top management and administration. Information Assurance and Cyber Security are integrated functions that require effective collaboration throughout the organization. It is imperative for security strategists to have everyone required on board, so that they know the value of the assets being protected and the real cost of breaches which can then help determine current and future security requirements.

© Happiest Minds Technologies. All Rights Reserved

Development process

The process of security strategy development can be depicted as follows:


Determine current state and define desired state
Perform Gap analysis with risk assessment
Determine resources and define constraints
Set control objectives and evaluate Control choices
Design controls with available resources
Design Monitoring and metrics for controls
Develop project management Plans

Organization, People, Process And Technology

The most important part of developing a security strategy is understanding the key elements of the specific business house. While it is essential to understand generic threats and vulnerabilities, the ones which can impact a particular organization is vital. Security strategists need to decide on how much effort, time and money is required to develop organization specific security policies and controls.

Industry guidelines such as COBIT may be used to plan and decide on the framework for aligning IT governance objectives, process definitions, high-level requirements for control management for each of those processes and management guidelines to help arrive at maturity levels.

A proper understanding of the organization's environment where business and IT goals are aligned, taking account of factors such as applications, databases, networks, information exchange and workflows in information management system, reporting, research and records management needs to be undertaken. The roles and responsibilities required for various positions within I.T and business needs to be documented. Identification of personnel with relevant skillsets, requirements for training to enhance or develop functional and technical competencies needs to be commenced. Awareness around concepts of integrity, confidentiality, and privacy is an essential component for any security strategy. Consistent efforts must be carried out to ensure that the workforce is adequately trained on these concepts and that people are fully aware of their role and responsibility in the organization lifecycle.

A detailed understanding of the various I.T processes such as demand, capacity, investment, human resources, quality, education and training, internal control, compliance, performance, operations, service, vendor, portfolio and SDLC etc., are required. Processes should be assessed for maturity prior to the security strategy planning and areas which require improvement must be identified. An action plan should be drafted ensuring the gaps are bridged through implementation of specific controls (logical and technical). Detailed understanding of how the information flows through the ecosystem, the type of data classification (if it exists) and characterization of such data, interoperability and information exchange is required to gain insight into the data management process.

Certain key requirements, such as, legal, regulatory, statutory, business and contractual needs to be identified and compared against internal processes, policies and procedures. Raising awareness through training campaigns and periodic assessments are extremely important.

External parties play a vital role in any organization. They can be internet service providers, attorneys, IT services such as application development, testing, maintenance, hardware support, managed services, device vendors etc. A comprehen-sive security strategy should include steps on how the external party must be assessed for security and compliance. The scope needs to include I.T, people and facilities in addition to how data is being collected, processed, stored and disposed within the organization. Documents that include the organization's policies, procedures, contract or agreement and reporting to service levels should be examined as well.

Assumptions, constraints and resources

While developing a security strategy, certain assumptions needs to be factored in. They can be planned projects by I.T and business teams, processes that are undergoing re-engineering or improvements, discussions on how personnel and budgets will be managed more effectively, the various groups or committees that will be formed for audit, security and risk management etc.

Constraints are limitations or restrictions or conditions that may prevent or diminish the achievement or implementation of a component or the entire strategic objective. Constraints can be contextual, be it legal, physical, ethical, policies, culture, costs, personnel, organizational structure, resources, capabilities, time and risk tolerance or operational - manageable, maintainable, efficient, effective, proportional, reliable, accurate and in-scope. These can also be the magnitude of effort, resources required for development, implementation, testing and support, challenges around legacy systems, integration with existing technologies, processes, changing or upcoming legislation and customer requirements. All applicable constraints must be identified during strategic planning process and taken into consideration for each objective.

Resources can be defined as any activity, process, asset, technology, individual, policies, procedures, standards, guidelines, architecture, controls, technology, personnel, roles and responsibilities, awareness etc; that can be utilized in some manner to move toward addressing a gap and thus serves in implementing the security strategy. Even if an organization is covered with firewalls one weak link in the chain can usher an attacker. Thus, the selection of appropriate security controls is an extremely important task having major implications on the operations and assets of any organization. Out of all resources, humans are mostly considered the weakest link and thus training and awareness should be an ongoing part of a comprehensive security strategy.

Information security is everybody's responsibility and not just the IT department. Many users within an organization limit themselves to following just the basic compliance. A successful security strategy must include every stakeholder within its fold and develop consistent processes and strategies motivating users to take ownership and help build a sound security policy.

Gap analysis and risk assessment

In order to determine the current state of information security governance attributes and characteristic, approaches from industry guidance such as COBIT, ISO-27001/2, CMM or other can be utilized. A detailed gap analysis or assessment is one of the essential steps in understanding the bridge between current and desired state. The following processes are generally followed:

Plan:

- Setting the context
- Understanding business goals, objectives, critical risk and success factors
- Identifying legal, statutory, regulatory and contractual applicability
- Defining the scope and boundaries for the exercise
- Preparing a project plan that includes schedule or timelines, information regarding stakeholders – internal, vendors or contractors, business units, processes, list of documents that must be reviewed, resources required and deliverables expected.
- Identifying assets – application, database, confidential and sensitive data, infrastructure devices, facility, people etc.
- Identifying threats and determine risk criteria based on current framework or industry best practices
- Preparing assessment questionnaire

Assess & Analyze:

- IT governance framework, risk management practices, business processes, I.T processes and organizational structure Review documentations such as policies, procedures, handbooks, manuals, previous audit or assessment reports, current security practices, I.T architecture and perform applications walkthrough
- Interview stakeholders based on assessment questionnaire, understand security awareness and adherence to requirements and controls
- Perform control assessment on identified scope
- Determine impact and likelihood of threats – source, nature, current controls, asset and data criticality, data sensitivity etc.
- Estimate identified risks and perform risk evaluation to compare against implemented controls, significance and mitigating factors

Report:

- Map current processes to controls
- Determine desired state
- Identify remediation activities, assign priorities and develop remediation plan
- Prepare draft report and review that with stakeholders
- Incorporate feedback and develop final gap analysis and risk assessment report

After completion of above activities, the next steps are as follows:

- The control objectives are tasks that address the risks identified during the previous stage and helps bring the current state to the desired state. Control objectives can be determined by examining the gap analysis and risk assessment report and aligning them with industry guidelines such as COBIT, ISO-27001/2 etc. Risk treatment options needs to be evaluated and a treatment or remediation plan developed to ascertain what risks need to be mitigated and to what extent. The residual risks, risk acceptance criteria along with legal, statutory, regulatory and contractual requirements and current controls implemented needs to be included while selecting control objectives.
- The next step would be to compile a list of controls that can be evaluated against available resources. Both contextual and operational constraints need to be determined and evaluated against these control choices and modified or replaced accordingly. In order to achieve the required assurance level, the control strength needs to be examined to determine the reliability and effectiveness and then a decision should be taken whether additional protection mecha nisms are applicable and or required.

© Happiest Minds Technologies. All Rights Reserved

- For each control choice, the applicable metrics and monitoring mechanism needs to be designed. Indicator concepts can be used for measurement of performance and effectiveness of goal accomplishment. These indicators enable the evaluation of process in alignment with business strategy. A security dashboard is essential and is primarily composed of dissemination of knowledge, measurement of processes and their maturity level, performance of critical processes, information for stakeholders, conformance level, surveillance of processes gap and alarming functionalities etc.

Management responsibility and expectations:

- The Chief Information Security Officer (CISO) should ideally be the strategic administrator and ultimately responsible for the creation, administration and communication of this security strategic plan. The CISO may assign other personnel as required to manage specific tactics or to facilitate strategic planning activities.
- The CISO may assign a manager from each business unit to look at a specific objective, as and when required. The assigned manager shall report progress on that tactic on, at minimum, a monthly basis, or more frequently depending on the requirement. .
- The strategic administrator needs to review, consolidate and communicate the progress of the strategic plan to personnel and business units on a quarterly basis at minimum

Each strategic objective will need adhere to the following tenants, goals, and objectives:

- Acquisition and implementation of common enterprise security tools to maximize cost reductions with economies of scale. Technologies, tools and solutions must be integrated to the maximum possible capacity providing automated enterprise-wide visibility into the security structure of the organization's information and information systems.
- Standardization decisions will need to be formally documented and the resulting standard or specific product in cases where there are no standards-based solutions available will need to be incorporated into the enterprise architecture technical reference model.
- Consideration should be given to leveraging and integrating existing investments to the greatest extent possible to conserve available constrained budgetary resources.
- Solutions should not be conceived in a fashion where consideration is given towards addressing only a single risk or requirement. Solutions should collectively be able to mitigate risks while addressing cost efficiency. .

Conclusion

Strategy implementation, testing and reviews are other activities should be planned as part of the development. Ideally, the executive committee and the Board needs to review the security strategy with the CISO, understand the implications and effects provide feedback on each initiative strategic objective and allow time for the CISO to respond to the comments and send the next version to the strategic committee for discussion, refinement and approval. The CIO and CEO should review, approve and communicate the final security strategy document to the intended audience. The CISO shall then officially publish the same to all relevant stakeholders. To measure success of the security strategy, one must ensure that initiatives provide enough flexibility to adjust to abrupt changes in business, legal and technical environments. The strategic task must generate a sense of eagerness among the personnel so that they follow the plan and take personal ownership ensuring its success. Managers and personnel need to be held accountable for the success or failure of their assigned initiatives and tactics. A security strategy is not a one-time activity and thus assessments must be done at least quarterly to measure effectiveness of implemented initiatives. It should be revised periodically reflecting changes in legislation, business and technology

© Happiest Minds Technologies. All Rights Reserved

About the Author

Ashok Kumar DL

Ashok Kumar DL is a seasoned InfoSec Consultant with rich experience in consulting, designing, implementing, assessing and managing large and complex InfoSec projects across industry verticals. He brings in over 13 years of experience in Governance, Risk, Compliance, Business Continuity, Identity & Access Management, Disaster Recovery, Privacy, Threat and Vulnerability Management.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact: business@happiestminds.com **Media Contact:** media@happiestminds.com

© Happiest Minds. All Rights Reserved.

E-mail: business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on

This Document is an exclusive property of Happiest Minds Technologies