CYBER DEFENSEDOCTIIPE
MANAGBING THE RBK FULL APPLIED GUDE TO ORGANATIONL ORGANIATILLY CYBER DEFENSE

Abstract – The analysis of the "Cyber Defense Doctrine that Manages Risks: a Complete Applied Guide to Organizational Cyber Defense" focuses on various aspects of organizational cyber defense, including risk management systems, elements of cybersecurity in military operations, incident response planning and the use of cyber defense tools and methods. Emphasizing the usefulness for cybersecurity specialists and specialists in various industries, the presented material can be considered as a guide that provides insight into the implementation of cyber defense strategies, improving the security level of an organization and developing a culture of cyber readiness.

It also serves as a valuable resource for information technology, forensics, law enforcement, and other sectors who require a deep understanding of cyber defense principles and practices. The document emphasizes the importance of a collaborative approach to cyber defense, and the need for continuous training and adaptation, taking into account constantly evolving cyber threats.

I. Introduction

The key points that give an idea of the doctrine are presented as follows:

- **Purpose (main)**: promotion Cyber Defense within the Israeli economy and is part of the national effort to protect civilian cyberspace
- **Purpose (secondary)**: aims to provide an orderly professional method for managing cyber risks in organizations. It helps organizations recognize relevant risks, formulate a defensive response, and implement a risk reduction plan accordingly.
- **Categories of Organizations**: The categorization of two types based on the potential damage from a cyber incident (Category A includes organizations with medium-to-low potential for damage, while Category B includes organizations with a high potential for damage).
- **Risk Assessment and Management Process**: different methods for risk assessment and management, depending on the organization's size, compliance with legal and regulatory requirements, and other parameters (e.g. with relatively small potential for damage up to USD 1.5 million and greater potential for damage).
- **Outcome**: organizations will understand their organizational risk map and what controls are needed to reduce those risks. These controls will form the basis for building the work plan, allocating resources, and preparing the organization accordingly.
- **Principles of Defense Doctrine**: management responsibility, defense from the adversary's view, defense based on Israeli knowledge and experience, defense in accordance with the potential for damage, and defense based on depth of implementation.

II. Principles of Defense Doctrine

The purpose is to establish a set of core principles that organizations should adhere to in order to effectively manage cyber risks and enhance their cyber resilience.

The intended audience for these principles includes organizational leaders, information security professionals, and cyber defense experts who are responsible for managing cyber risks and implementing defense strategies within their organizations

A. Automation and Integration process

The document emphasizes the importance of automation and orchestration processes in defense doctrine:

- Automation and orchestration processes reduce the need for human involvement in defense and operational processes, thereby minimizing the likelihood of human error and reducing the level of exposure of various bodies to personal information
- The document suggests adopting the MITRE ATT&CK ontology to use advanced automated solutions for continuous and ongoing control and execution of response processes. This would limit human manual involvement to exceptional cases
- proactive defense actions should be taken to preserve information. This includes maintaining effective capabilities for dealing with information leakage events, such as acquiring the ability to remove information that has been leaked to the Internet and Darknet
- The document emphasizes that the Chief Information Security Officer (CISO) plays a significant role in protecting information and privacy, and must harness the various bodies within the organization to maximize the level of defense
- The defense doctrine controls are incorporated into a framework that includes aspects of identification, defense, detection, response, and recovery. Through the

implementation of cyber defense recommendations and information security, aspects that serve the defense of privacy are interwoven into the controls themselves

- The concept of defense required to address advanced threats includes advanced approaches. Using these approaches will help the organization achieve advanced capabilities, such as validation and deception in order to gain time, exhaust the attacker, and even create deterrence against potential attackers

B. CISO Role

The CISO plays a critical role in protecting information and privacy within an organization. This includes understanding and complying with privacy laws, balancing different interests, managing risk, guiding defense strategies, and implementing controls effectively:

- **Protection of Privacy Law**: It states that any infringement on privacy must be carried out in accordance with the law and general principles of reasonableness and good faith.
- **Balancing Interests**: The CISO must strike the right balance between different interests to enable informed decisions within the organization. This includes considering aspects of privacy and compliance with principles such as Security by Design, Privacy by Design, and Threat Informed Defense
- **Risk Assessment and Management**: a process for risk assessment and management includes defining main defense objectives, identifying defense gaps, and building a work plan to minimize these gaps. The CISO plays a crucial role in this process
- **Management Responsibility**: The responsibility for protecting information primarily lies with the management of the organization. The CISO is a key figure in ensuring this responsibility is met
- **Defense from the Adversary's View**: The CISO should understand common attack scenarios and the effectiveness of defense recommendations against them. This understanding informs the weight and priority of defense recommendations
- **Defense based on Potential Damage**: The investment in protecting each defense target should be in accordance with its level of criticality for the organization's functioning. The CISO should guide this investment
- **Defense based on Depth of Implementation**: it encourages organizations to implement controls at different levels of maturity. The CISO should examine controls according to their implementation effectiveness
- **Organizational Classification**: a classification system for organizations based on the potential damage from a cyber incident. The CISO should understand where their organization falls within this classification system to guide their defense strategy.

III. THE PLANNING PROCESS IN THE ORGANIZATION’S VIEW

The planning process in an organization's view is a method for managing cyber risks within an organization. The purpose of this process is to help organizations identify relevant risks, formulate a defensive response, and implement a risk reduction plan accordingly

The intended audience for this process includes managers and experts in the fields of information security and cyber defense.

The different methods should be used for risk assessment and management, depending on the organization's size, compliance with legal and regulatory requirements, and other parameters, e.g. according to organization categories. Category A organizations are those where the scope of damage caused by a cyber incident does not exceed USD 1.5 million, while Category B organizations are those where the extent of the damage caused by a cyber incident may cost more than USD 1.5 million.

The process for Category A organizations includes a simple and quick process of mapping Defense objectives and answering a limited number of questions, which are tailored to organizations from this category. Usually, the process is carried out through an external party which accompanies the Cyber Defense aspects of the organization

The process for Category B organizations includes a process of Risk Assessment, understanding the required Defense response to the Risk Matrix and Risk Appetite, examining the current situation in the face of industry-accepted Defense recommendations (Gap analysis) and formulating a work plan for the mitigation of risks (Mitigation Plan) or other risk handling measures

The final product after working with it is that the organization will understand the organizational risk map, and what controls are needed to reduce those risks - including the right priorities for implementing the work plan. These controls will form the basis for building the work plan, allocating resources, and preparing the organization accordingly

A. Key components of the planning process

The key components of the planning process in the organization:

- **Demarcation of Activity**: This involves understanding the organization's digital assets and where they are stored, which is crucial for identifying what needs to be protected against cyber threats.
- **Risk Assessment**: This includes identifying relevant risks to the organization, analyzing these risks, and assessing them to understand their potential impact and likelihood.
- **Handling the Risk**: Organizations must decide on a strategy for dealing with identified risks. This could involve accepting, reducing, transferring, or avoiding the risks.

- **Building a Work Plan**: Once risks have been identified and a strategy for handling them has been determined, the organization must develop a work plan to address the risks. This plan may include implementing processes, procuring solutions, and training employees.
- **Continuous Auditing and Control**: The implementation of the work plan should be periodically reviewed to ensure its effectiveness and relevance. This includes checking for new information assets, implemented controls, and required management inputs.
- **Involvement of Legal Adviser**: The organization's Legal Adviser should be involved early in the planning process to ensure compliance with legal and regulatory requirements and to be integrated into key decision-making processes.
- **Decision-making Supported by Evidence**: The organization must use independent security circles to cope with various threats and ensure that decision-making is supported by evidence, which will provide a realistic picture of the security situation (Security Posture).
- **Minimizing Privacy Invasion**: The Defense Doctrine control structure offers the CISO extensive freedom of action to reduce the level of risk to an acceptable value while minimizing the invasion of privacy.

IV. Implementation of the Doctrine of Defense

A. Main points:

- It emphasizes the importance of automation and orchestration processes to reduce human error and exposure to personal information
- It encourages the use of advanced automated solutions for continuous control and execution of response processes, with human involvement only required in exceptional cases
- Proactive defense actions should be taken to preserve information, in addition to maintaining effective capabilities for dealing with information leakage events
- The Defense Doctrine controls are incorporated into a framework that includes aspects of identification, defense, detection, response, and recovery
- It encourages organizations to implement controls at different levels of maturity on issues such as SOC (Security Operations Center), DLP (Data Loss Prevention), or risk surveys
- It allows for a focus on the risks relevant to each organization, with periodic audits and intelligence assessments carried out throughout the entire Israeli economy
- The investment in protecting each defense target in the organization will be in accordance with its level of criticality for the organization's functioning

B. Level control difference

Basic level control usually indicates a process that exists but is not managed and is executed manually. It's the starting point for organizations, allowing them to implement basic controls before moving on to more advanced and complex controls

On the other hand, innovative level control indicates the implementation of control in a managed, documented, automatic, efficient, and effective manner. This level of control is more comprehensive and takes into account the organization's constraints, information classification, and adaptation to business processes

V. Implementation of the Doctrine of Defense for a Category A Organization

It outlines a five-stage process for implementing a defense doctrine in a category A organization.

- **Stage 1: Demarcation of the activity**: This stage involves defining the scope of the organization's activities that need to be protected.
- **Stages 2 and 3: Assessing the risks and determining a strategy for dealing with them**: These stages involve identifying potential risks to the organization and developing a strategy to manage these risks.
- **Stage 4: Building a work plan**: This stage involves creating a detailed plan for implementing the defense strategy.
- **Stage 5: Continuous auditing and control**: This stage involves ongoing monitoring and control to ensure the effectiveness of the defense strategy and to make necessary adjustments

VI. Implementation of the Doctrine of Defense for a Category B Organization

It outlines a five-stage process for implementing a defense doctrine in a category B organization.

- **Stage 0 – Corporate governance and strategy for corporate risk management**: This stage involves establishing a governance structure and strategy for managing corporate risk. It sets the foundation for the organization's approach to cyber defense.
- **Stage 1 – Demarcation of activity and risk assessment survey**: This stage involves defining the scope of the organization's activities and conducting a risk assessment survey. This helps the organization understand its potential vulnerabilities and the risks associated with its activities.
- **Stage 2 – Risk Assessment**: This stage involves a detailed assessment of the risks identified in the previous stage. The organization evaluates the potential impact and likelihood of each risk, which helps in prioritizing them for mitigation.
- **Stage 3 – Handling the risk**: After the risks have been assessed, this stage involves developing strategies to manage them. This could involve mitigating the risk,

transferring it, accepting it, or avoiding it, depending on the nature of the risk and the organization's risk tolerance.

- **Stage 4 – Building a work plan**: Based on the risk handling strategies developed in the previous stage, this stage involves creating a detailed work plan. This plan outlines the steps the organization will take to implement its risk handling strategies.
- **Stage 5 – Continuous auditing and monitoring**: This final stage involves ongoing auditing and monitoring to ensure that the risk handling strategies are effectively implemented and to identify any new or changing risks. This ensures that the organization's approach to cyber defense remains effective over time

VII. Areas of defense

There are five main areas into which cyber defense is divided are:

- **Identify**: This function involves developing an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect**: This function outlines appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**: This function defines the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**: This function includes the appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover**: This function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

These functions were built in accordance with the NIST Cybersecurity Framework (CSF), which provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

A. NIST Relationlink

The document uses the NIST CSF as a basis for its Control Bank. The Control Bank is a centralized set of cybersecurity recommendations divided into five main areas of cyber defense: Identify, Protect, Detect, Respond, and Recover.

The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices designed to help organizations manage and reduce cybersecurity risk. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. The framework is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

These areas align directly with the five functions of the NIST CSF.

- **Identify** – Develop an understanding of how to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Implement safeguards to ensure delivery of critical services.
- **Detect** – Identify the occurrence of a cybersecurity event.
- **Respond** - Act regarding a detected cybersecurity incident.
- **Recover** – Maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

VIII. Appendixes

Key principles include the principle of consent, which gives customers control over their personal information, and the principle of goal proximity, which stipulates that information can only be used for the purpose for which it was originally collected. It also outlines obligations regarding the registration of databases and their security, including the need to periodically review the necessity of retaining information based on its original collection purpose

A. Organization Defense Controls

In the context of Category A Organization Defense Controls with an emphasis on computers, the document outlines several key points and findings:

Evidence Requirement: The document emphasizes the need for proper documentation to ensure that the controls are correctly integrated into the organization. This data can also serve as a basis for regulation and/or accreditation/certification

Ranking and Setting Priorities: The controls have been classified on a scale from 1 to 4. Level 1 controls are the most basic and are required of any organization for each asset, while level 4 controls are only required for a Defense target whose potential for damage is 4

Continuous Control: Continuous control is essential to the organization as it allows the Cyber Defense party within the organization to understand what the Defense gaps are and what steps are required to improve the situation. Continuous control can be performed at the compliant level, addressing defined issues and controls, or by measuring risks, threats, readiness for attack scenarios, and more

Key Performance Indicators (KPIs): KPIs allow the organization to measure and quantify the level of Defense at a given time, comparing it to the measurement history, thus examining the trend

Risk Assessment and Management Process: Cyber Defense activities are carried out due to the organization's desire to manage the cyber risks to which it is exposed. The organization will first define what its main Defense objectives are, what level of Defense is required, and what are the Defense gaps compared to the desired situation, and then proceed to build a work plan to minimize the gaps

Final Product: After working with this document, the organization will understand the organizational risk map, and what controls are needed to reduce those risks - including the right priorities for implementing the work plan. These controls will form the basis for building the work plan, allocating resources, and preparing the organization accordingly

B. *Control Bank*

The Control Bank is a critical tool for organizations to systematically address cybersecurity risks by implementing recommended controls tailored to their specific needs and threat landscape. It serves as a guide for organizations to prioritize and implement cybersecurity measures effectively.

- **Purpose of the Control Bank**: The Control Bank is designed to centralize Cyber Defense recommendations in various areas and update them frequently based on technological developments and emerging threats.
- **Gap Analysis**: The Control Bank is used for mapping all the gaps versus the list of different controls, helping organizations understand where they are not properly organized and to get a list of gaps. This process is compliance-oriented and results in a list indicating whether controls are "correct/incorrect/irrelevant/partially implemented".
- **Individual Mapping**: Controls are individually mapped against threats and critical risks in organization-sensitive Defense targets. This acknowledges that the implementation of controls is a dynamic process that varies from one Defense objective to another, and certain Defense objectives may require detailed examination of controls like monitoring, supply chain management, and backup existence.
- **Transition to Risk-Based Perspective**: The use of the Control Bank facilitates the transition from a compliance-oriented perspective to a risk-based perspective, aligning the implementation of controls with the organization's management vision and reducing risks and individual threats.
- **Unique Characteristics of the Control Bank**:
  - **Focus on High-Value Controls**: The Control Bank focuses on controls that make the most contribution to Defense, where the "cost versus benefit" is the highest.
  - **Depth of Implementation**: Controls can be implemented in various forms, ranging from manual and non-systematic implementation to built-in implementation backed by full automation capabilities and up-to-date professional knowledge.
- **Support for Audit Processes**: The Control Bank supports audit processes and helps prepare the infrastructure for accreditation and certification by providing a structured set of controls with clear definitions for implementation depth and required evidence.

C. *Tools and methods for implementing continuous control in the organization*

The focus on continuous control underscores the dynamic nature of cyber threats and the need for organizations to regularly assess and adjust their defense postures.

- **Continuous Control as a Compass**: Continuous control is essential for an organization as it provides a reflection of the current state of cyber defense and guides what steps are required to improve the situation. It allows the Cyber Defense party within the organization to know the defense gaps and the necessary steps for improvement.
- **Compliance Level Control**: Continuous control can be performed at the compliance level, addressing defined issues and controls, such as the compliance status in Defense Doctrine controls.
- **Risk and Threat Measurement**: It can also involve measuring risks, threats, readiness for attack scenarios, and more, going beyond mere compliance.
- **Defining Measurement Parameters**: To build an internal plan for continuous control management, the organization must first define a number of measurement parameters.
- **Automated Mechanisms**: Mechanisms should be implemented that will absorb the measurement results and present the current situation alongside the trend in the organization. Automation is crucial for this process.
- **Key Performance Indicators (KPIs)**: KPIs allow the organization to measure and quantify the level of defense at a given time, comparing it to the measurement history, thus examining the trend. These metrics may examine various aspects of cyber defense.