CHAPTER A – COMPANIES INTRODUCTION

1 COMPANIES OVERVIEW

Tailor made security solutions has enabled the formation of an international group specializing in the preventing and minimizing risks to clients' reputation, property and information.

Corporate espionage, identity theft, electronic weapons, good vs. evil – a frightening reality. Malicious greed, vicious hunt for profit, insatiable hunger for inside information at all costs, brilliant hackers mercilessly striving for personal gain…money, lots of money…your money.

With unrivalled expertise, resourcefulness, and brilliant operational risk management and information security services, we deliver cream-of-the-crop, airtight security coverage for your critical organizational assets.

TMS a Top global leader in consulting for, facilitating and managing information security, antifraud, risk management, revenue assurance, and loss prevention project, as well as in business continuity planning and state-of-the-art technology services. we have acquired worldwide recognition thanks to an exclusive portfolio of unique, value-added innovated solutions and first-class implementations.

Leveraging over a decade of accumulated knowledge and outstanding expertise in leading complex projects of international scale in a variety of industries in both the private and public sectors, TMS solutions – now a leader in the information security industry – continues to set new standards as the number one provider of information security solutions.

Our integrity, originality, cutting-edge professionalism and unique ability to translate business requirements into technological solutions are the keys to our competitive edge.

TMS security solutions, we employ highly skilled professionals with vast experience in multiple vertical markets and unmatched understanding of leading technologies. We apply proprietary methodology and a cost-benefit approach to contain operational risks and threats within acceptable limits. We provide not only first-class professionalism, but also leadership.

We offer a unique approach to security management and we deliver. Always.

Integrity, resourcefulness, worldwide established knowledge and cutting-edge professional expertise, optimal compatibility to your business needs…are only some of the attributes distinguishing us from the competition.

Main benefits;

- ***We take a proactive approach***: We do not wait and then react – we asses, strategize and implement preemptive tools designed to provide you state-of-the-art professional solutions.
- ***We rely on unparalleled professionals*** with vast experience in multiple vertical markets.

- ***We are dedicated to our customers***: We understand how difficult it is to "give the keys to the kingdom" to an external service provider.
- ***We employ proprietary methodology*** encompassing technical and non-technical security measures with a cost-benefit approach.
- ***We have proven top-quality skills*** in building suitable infrastructures as a preliminary step towards managing security, combined with a complete set of operational tools.
- ***We are committed to excellence and delivery on our commitments:*** For us, customer satisfaction is the reward for impeccable services and the foundation for mutual success.
- ***We live in the hacker world***: We share our knowledge with our customers, we document our activities and prove to our customers that their system is vulnerable; we deliver real solutions to real problems.
- ***We offer unique proficiency in the technology and methodology of application security***, together with unconventional (some say criminal-like) thinking and keen understanding of the operational patterns of malicious hackers.
- ***We are willing to do whatever it takes to make you satisfied***.
- ***We create a complete information security apparatus*** by transferring skills and technology accompanied by an accelerated information security learning curve, enabling clients to sustain long-term low risk levels.

Our group has proven success in:

- Establishing a Cyber-Terrorism Unit
- National Cyber Security Exercises - Table top cyber security exercises (wet / dry)
- Cyber threat intelligence - studies based on open sources (OSINT), using off-the-shelf tools to assess threats to the client.
- Cyber threat survey – (Physical, logical & human resource).
- Advance Persistent Treats (APT) Attacks
- Zero day, DDoS, Widespread Virus Outbreak and other custom malwares – design, programing and attacks (including CLS systems).
- Assessing cross-organizational preparedness (resilience tests, including controlled penetration tests to identify vulnerabilities on all levels).
- Cyber incident management, reporting and investigation policy
- Cyber Security Operation Center (CSOC) - establishing an operation center.
- Critical Infrastructure – CIP \ SCADA
- ISO Compliance - ISO 27032: Cyber Security compliance.
- Developing and implementing antifraud policies, processes and technical solutions

- Implementing Revenue Assurance processes and solutions
- Designing intricate security infrastructures
- Implementing integrated technologies
- Application Security: Complex penetration tests, Code Review, implementation of cutting-edge Web Application Firewalls (WAF), secure architecture design, secure development and related training.
- Designing and implementing multipart security projects (Identity Management (IdM), Public Key Infrastructure (PKI) and Security Operation Center (SOC))
- Designing security architectures and topologies
- Developing anti-hacking solutions
- Spearheading data communication security solutions
- Fraud Management, Revenue Assurance and information security training

Our proven success in;

Tms
Tailor Made Security Solutions

Cyber

Establishing Cyber security units :

providing security forces with Cyber defense capabilities from A to Z, meaning that we study the organization and its needs, provide a holistic technical and operational solution based on vetting the needed personnel, assist with comprehensive organization structure and operational procedures based on our long operational experience and continue with coaching of the cyber forces after final establishment and delivery to ensure the continuity of its operational and technical capabilities, providing updated threats analysis and technical capabilities and know how.

CHAPTER B – NATIONAL CYBER COMMAND

2 CYBER PROJECT

"Cyber – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society." A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy."

The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others.

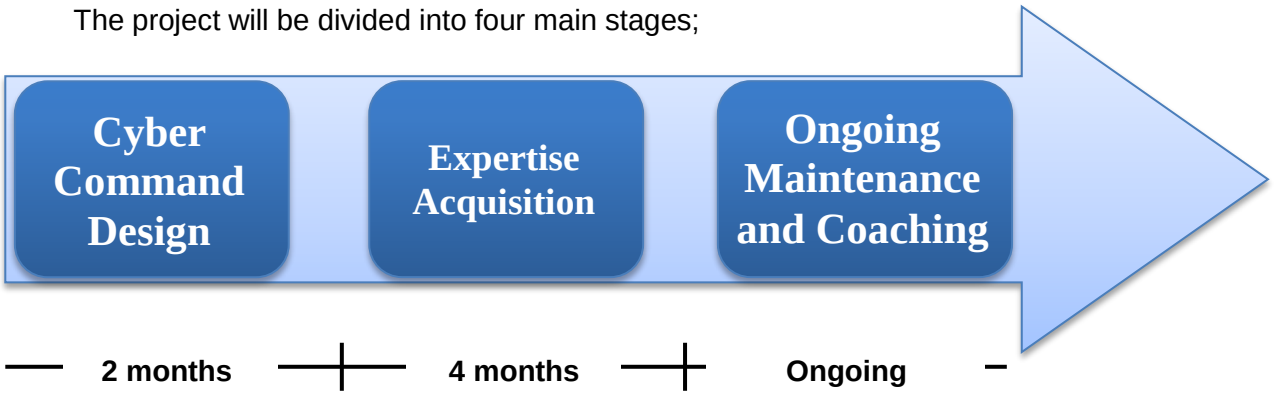
2.1 PROJECT VISION

The project vision is to establish a Cyber Security Operation Unit that will enable the ability to improve preparedness in dealing with the current and future challenges in cyberspace against cyber-attacks (detection, prevention, forensic), improve the security level and raise the security awareness, build their own pro-defense capabilities and set up the national cyber security policy, methods, and governance.

2.2 PROJECT METHODOLOGY

Dealing with cyber and infosecurity threats requires attention to and integration of multiple, interrelated aspects into a single whole to provide a comprehensive solution. The project methodology outlined herein is the best practice methodology designed on the Israeli and national scale similar projects.

The project will be divided into four main stages;



Stage 1: Cyber Command Design

This preparatory stage is particularly important in the current project, due to our lack of familiarization with your organization. At this stage, we propose to study your requirements, objectives, infrastructures, systems and processes and identify risk areas in order to delimit the project scope and decide on the Cyber Command main departments and activity areas. For example, not all Cyber Commands conduct active defense.

To do so, we will:

- Meet with relevant personnel
- Conduct a technological study of your IT infrastructure (existing or future)
- Review existing methods and human resources

Stage 1 Activities:

A. Specifying project goals and objectives, studying client requirements and identifying the key stakeholder in the project

B. Selecting the steering team of the project

C. Defining the Cyber Command scope of responsibilities and authorities

D. Specifying the main areas of interest such as:

- Enemies and Potential Targets
- Intelligence (espionage, wiretapping, data collection)
- Hacking and APT
- Denial of Service
- Fraud
- Sabotage
- Identity Theft
- Viruses and Malwares
- System Control
- Toolbox
- Forensics

E. Meetings with relevant personnel to study the following:

- The organization's infrastructure architecture
- Interfaces with other organizations
- Infrastructure management
- Security measures to protect the organization's external connections
- Security measures to protect the organization's internal systems
- Main focus areas

F. Detailed study of existing technology and processes:

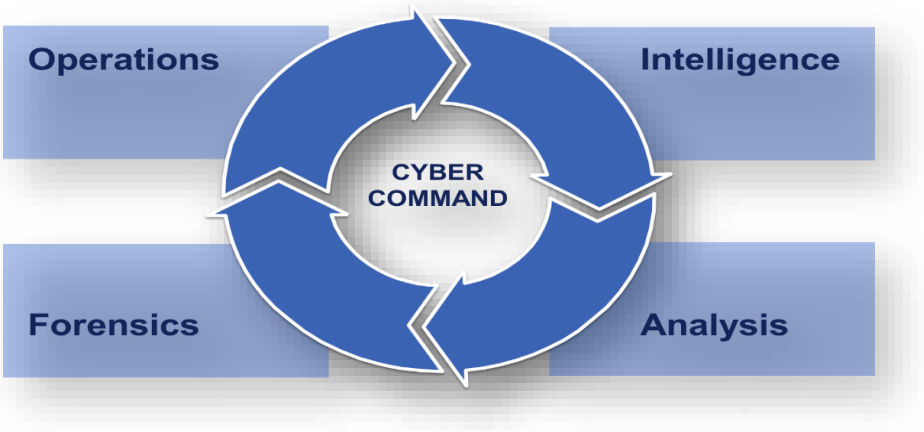
- Technologies already used by the organization, and where
- Technological safeguards
- Existing technical procedures and processes – hacking and APT's techniques, knowledge bases, basic steps and other processes.

- Full-scale, multilevel (departmental to global) assessment of your operations to identify and prioritize specific areas

G. Full-scale, multi-level (departmental to global) assessment of your operations to identify and prioritize specific areas. The focus will be on: Existing policies, systems, procedures and automated processes, Internal risks specific to your operations, External risks specific to your operations.

Stage 2: Acquiring Expertise

This stage will begin with the knowledge and educational acquirement. We will conduct several trainings (according to the Cyber Command design and the client requirements), conveying our experience and knowledge and equipping the CDC with all the necessary tools.

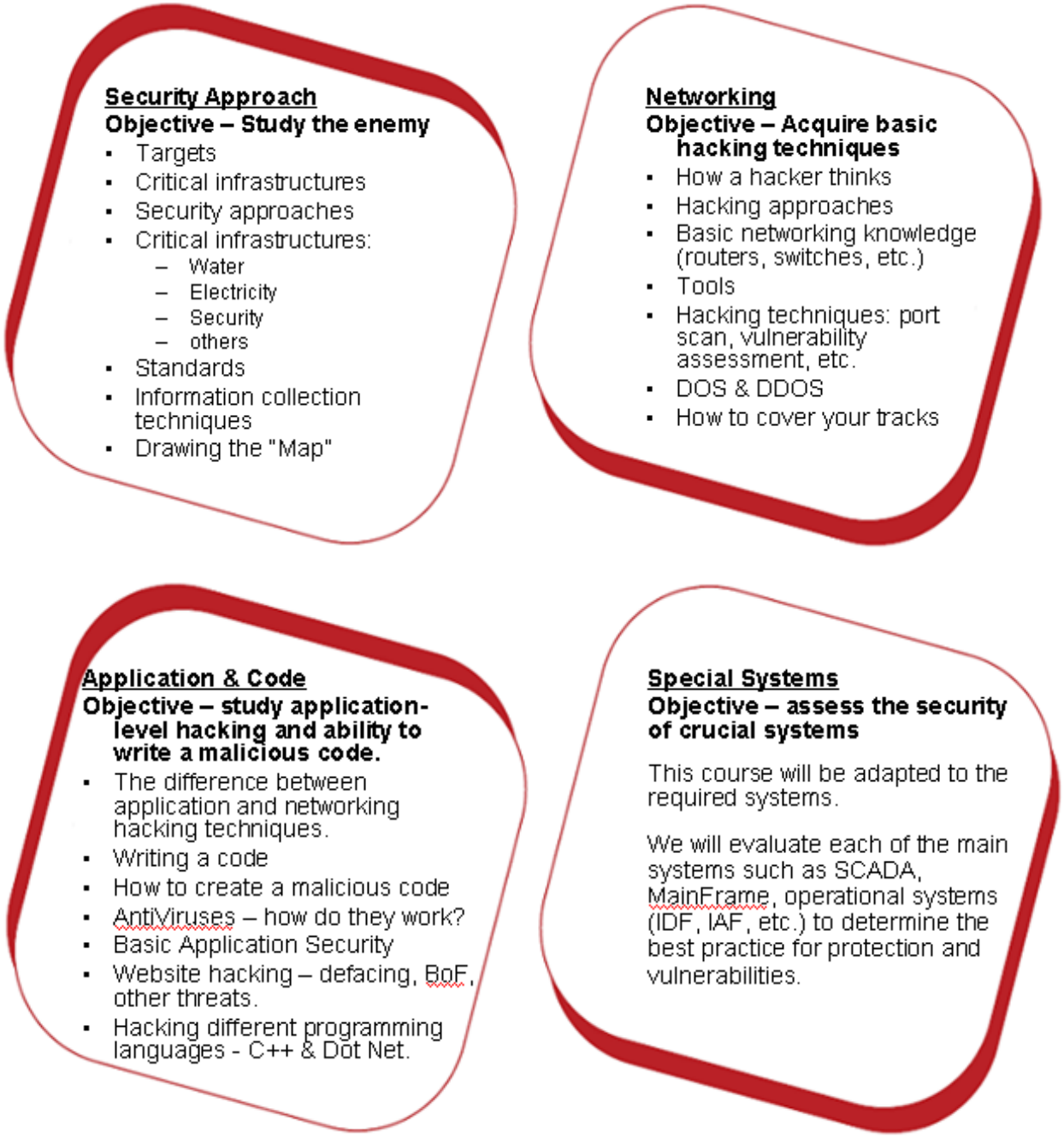


Stage 2 Activities:

Operations:

- Trainings (course syllabus presented in annex A)
  - Information Security Basic course
  - Advance Security Course
  - Blue Team – how to protect from being hacked, what are the hacking and APT's techniques. At this stage we will offer course focused on the following domains:
    - Security Approach – How do other defense organizations protect themselves?
    - Networking
    - Application including writing a code
    - Special systems – critical utilities: electricity, water, and others (such as SCADA)

Cyber



- Hands-on experience
  - Lab testing – one of the most important activities – a lab will be installed and we will conduct "war games" according to each scenario.
  - Honeypots – we will learn how to create a honeypot and how to recognize one.

- Covering your tracks – we will study and practice how to erase tracks and how to leave a backdoor.
- Viruses and Trojan horses – we will create a malicious code and test it against several anti-viruses.
- Intelligence collection.
- Designing a secure environment – we will design a secure environment according to the relevant scenarios.

- Tools implementation
  - Implementation of relevant tools (purchase, design, training, implementation, QA and documentation).

Forensics:

- Training
  - Basic forensics course
  - Advanced forensics course

  Course Contents:
  - Computer forensics guidelines
  - Forensic history
  - Where to find relevant information
  - Media storages
  - Evidence – laws and regulations
  - Evidence authenticity
  - Forensic tools such as Encase
  - Information collection methods
- Hands-on experience
  - Lab testing – a lab will be installed to forensic several cases
  - How to detect erased tracks
- Tool implementation
  - Implementation of relevant tools (purchase, design, training, implementation, QA and documentation).

Data Collection (basic training)

- Training

Basic Data Collection Course

Research – how to collect info on/offline; Resources – Internet / Phone lines / etc.; Business Intelligence – BI, audit info – analyzing audit logs; Blogs; Underground communities; Tools; Connectivity to other intelligence systems.

Intelligence (optional)

- Training

  Data Intelligence Course

  The main objective of this course is to teach how to anonymize information and handle anonymized information

  - Encryption algorithms
  - Stenography
  - "Read between the lines" – how to analyze a text and understand the hidden message
  - Encryption / Decryption
  - Data anonymization techniques
  - Website – honeypots
  - Website / Mail – sending an innocuous message (hidden message)
  - 3rd party – how to use a third party as your messenger – masking.
- Hands-on experience
  - Lab testing – a lab will be installed where we will practice encryption, decryption, masking and other techniques.

- Tool implementation
  - Implementation of relevant tools (purchase, design, training, implementation, QA and documentation).

2.3 PROJECT WORKPLAN

This is a high level work plan, a detailed one will be submitted after we will study the organization and will be able to collect the entire requirements.

2.4 Activities and Products by Stages

Stage	Duration	Final Products
Stage A - Unit Design	**2 Months**	▪ A Gap Analysis between the required status and the current. ▪ Scope of Work (SOW). ▪ High level Unit design document ▪ Low level Unit design document ▪ Unit positions and responsibilities
Stage B - Expertise Acquisition	**4 Months**	▪ Training books ▪ Scenarios ▪ Policies and procedures

2.5 Project Management

As the project suggested herein is highly complex, it will be lead and managed by a certified PMPs according to PMBOK

Excellence project management meets the ISO9002 standards and lead by a certified Project Manager. Project management will include all of the required tasks, such as;

- *Preparation meetings* – alignment of objectives, expectations, and reports, detailed work plan, schedule, etc.
- *Work plan* – detailed work plan in MS Project format prepared on a weekly basis, including tasks, position and experience, task content and deliverables and project staff and their experience.
- *Status meetings and presentation* – on weekly basis accompanied by a meeting summary. The status meeting will include status summary, actual versus planned status, future steps, critical breaches, etc.

2.6 Team

The project team will be composed of a Project Manager and eight different experts, which are the leading experts in this field. Their names and CV's will be submitted after contract signing.

2.7 Organization Resources

In order to ensure coordination and provision of all requirements, guarantee minimal disruption of on-going work, retain know-how and achieve mutual fulfillment the client is hereby requested to nominate a liaison to work with Excellence on a part-time basis during the project.

Annex A - CYBERSECURITY COURSE SYLLABUS

Course syllabus (example):

Chapter A – Introduction

1. Introduction to Hacking
1.1 Methodology
1.2 Full Disclosure
1.3 Ethics
1.4 Hacking & the Law
2. Cryptography
2.1 Stream Ciphers
2.2 Block Ciphers
2.3 Hash Algorithm
2.4 Weaknesses
2.5 Cryptographic Protocols
2.6 A-Symmetric Encryption
3. Linux
3.1 Basic Commands
3.2 Users & Groups
3.3 Permissions
3.4 Working with terminal
3.5 Compile & Execute

Chapter B – Reconnaissance

4. Introduction to Reconnaissance
4.1 Goals
4.2 General Understanding
5. OSINT
5.1 Google Hacking and Dorking
5.2 Site Mapping
5.3 Maltego Work Environment
5.4 General Relevant Information
5.5 Shodan
5.6 Whois Interrogation
5.6.1 IP Assignments with ARIN
5.6.2 Client
5.6.3 Methodology
5.7 Other Online Research
6. Organization Details
7. Enumeration
7.1 SMTP Enumeration
7.2 SNTP Enumeration
7.3 NetBIOS Enumeration

Chapter C – Network Attacks & Penetration

19. Wi-Fi
19.1 Introduction
19.2 Understanding 802.11x
19.3 Introduction to Tools
19.3.1 airmon-ng
19.3.2 airodump-ng
19.3.3 aireplay-ng
19.3.4 airebase-ng
19.3.5 Kismet
19.4 Cracking Encryptions
19.4.1 WEP
19.4.2 WPA
19.4.3 WPA2
19.4.4 WPS
19.5 WPS – reaver
19.6 Bypassing MAC filtering
19.7 Rouge Access Point
19.8 Netstumbler
20. RFID
20.1 Understanding RFID
20.2 Communication via RFID
20.3 Cracking and maintaining
21. Bluetooth
21.1 Enumeration
21.2 Basic tools
21.3 Bypassing security codes
21.4 False associations

Chapter F – Web and Web Application Penetration

22. Introduction
23. Tools
23.1 Firebug
23.2 Tamper Data
23.3 Paros
23.4 WebSCrab
23.5 Dirbuster
23.6 Fuzzers
23.7 Webshag
23.8 W3AF
24. Web Attacks
24.1 SQL Injection
24.1.1 Introduction
24.1.2 Blind
24.1.3 Error based
24.1.4 Union based
24.2 XSS
24.2.1 DOM based
24.2.2 Stored

24.2.3 Reflected
24.2.4 CSRF
24.3 Directory listing
24.4 Broken Authentication
24.5 Failure to restrict URLs
24.6 Insecure storage
24.7 Mal-configuration of Permissions
24.8 Changing User-Agent
24.9 File upload
24.10 LFIs
24.11 RFIs
24.12 PHP shell files
24.13 Sessions HiJacking
24.14 Sessions SideJacking
24.15 HTTP poisoning
24.16 Cross-Site Cooking
24.17 Session Fixiation

Chapter G – Exploitation

25. Introduction
25.1 What Is Exploitation
25.2 Types of Exploitation
25.3 0 Days
26. Buffer over Flows
26.1 Introduction
26.2 Finding Bugs
26.3 Case Studies
26.4 Verifying the Overflow in the STOR
26.5 Which Bytes Overwritten EIP
26.6 Diving Deeper
26.7 Shell Codes
27. Metasploit Framework
27.1 MSF Console
27.2 MSF Web
27.3 MSF CLI
27.4 Meterpreter
27.5 Meterpreter Commands
27.6 Payloads
27.7 Auxillary
27.8 Modules
27.9 Write an Example in Ruby

Chapter H – Reverse Engineering

28. Introduction
28.1 What is reverse engineering
28.2 Static analysis
28.3 Dynamic Analysis

Chapter I – Virology