CYBERGATE

Whitepaper

# Cybersecurity Capability Maturity

WE HAVE THE IN-HOUSE DEPTH AND BREATH OF
INFORMATION AND CYBER SECURIT

## About Us

CyberGate Defense (CGD) is a solution provider for the full spectrum of Cyber Security Defenses including Identify, Protect, Detect, Respond and Recover. Our objective is to provide cyber security services that would improve the overarching cyber security posture of the nation especially how Government departments offer its IT services and improving the cyber maturity of the critical infrastructure industries.

We also provide an outline approach for developing a Cyber Security Strategy in collaboration with the Government by clearly presenting goals and vision and detailing how that vision can be achieved.

## Our Vision

Building UAE's cyber security resilience through effective use of technology, processes and the local people.

## Our commitment

We believe that a cyber security provider can be about more than just the profits it makes, that by doing things the right way we can be a powerful force for good and safe environment where people and business communicate in cyber space with harmony.

By developing your strengths and enabling you to participate securely online, we'll help you to fulfil your security posture and getting the most from your IT investment.

## What is Cyber Security?

According to the ITU, the United Nations specialized agency for information and communication technologies; Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets.

## Cyber Security Challenges

There is a growing concern of cyber-attacks on individuals, businesses, governments and the heavy industry which our modern lives depend on. There is a tangible risk of these systems being vulnerable and targeted. Governments are targeted by Advanced Persistent Threats (APT), by groups or nation state that are willing to employ time and resources to attack a specific system. For these kinds of attacks, there is a strong likelihood that a compromise will have national security implications.

## Why we are different

Beyond our significant local presence, we have the in-house depth and breadth of information and cyber security expertise required to respond to the most technical information security challenges related to both Information and Operational Technology.

The principal reasons why East Gate Cyber Defense is the right partner to assist you with any cyber security undertaking are:

### Geographical:

Emirati Owned Company, headquartered in the UAE since 1987. Over the years East Gate provided the UAE Government with high intelligent services and solutions. Today the scope of our services has been extended to include cyber security solutions aimed to strengthen the nation from cyber-attacks.

### Sector Experience:

We currently operate in the Government sector providing value-added services and built solutions across the entire spectrum of cyber defense.

## Security Expertise:

Our multidisciplinary team of information and cyber security professionals includes internationally renowned experts in the fields of protecting the critical infrastructure, industrial control systems, information systems and networks.

## Contents

## What's Cybersecurity Capability Maturity? What are we trying to protect?

The Cybersecurity Capability Maturity Model addresses the implementation and management of cybersecurity practices associated with information technology (IT) and operational technology (OT) and the environments in which they operate. Our service makes it possible for organization to evaluate and make improvements to their cybersecurity programs.

## Our Approach

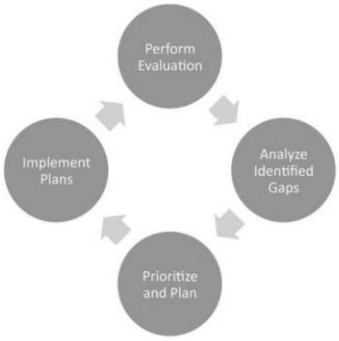
We follow a maturity model which includes a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. Our engagement will help strengthen cybersecurity capabilities in the ONG subsector. Using the model, we evaluate cybersecurity capabilities consistently, to communicate these capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments.

- Enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable ONG organizations to prioritize actions and investments to improve cybersecurity

We do this by employing a set of evaluation methodology and toolkit to measure and improve its cybersecurity program. We will provide a descriptive rather than prescriptive industry focused guidance.

We will engage with you on different level to maximize the benefit and to guarantee a successful outcome. The following members can participate in the program:

- Decision makers (executives) who control the allocation of resources and the management of risk in organizations; these are typically senior leaders
- Leaders with responsibility for managing organizational resources and operations associated with the domains of this model
- Practitioners with responsibility for supporting the organization in the use of this model (planning and managing changes in the organization based on the model)
- Facilitators with responsibility for leading a self-evaluation of the organization based on this model and the associated toolkit and analyzing the self-evaluation results.



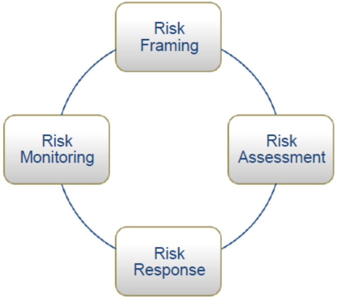
## Benefit

Evaluate cybersecurity capabilities consistently, communicate capability levels in meaningful terms, and prioritize cybersecurity Investments.

Establish and maintain plans, procedures, and technologies to detect, identify, analyses, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

## Relationship to the Risk Management Process

The following model will be used as part of a continuous enterprise risk management process.



## Deliverable

- ➢ Produce a high level of abstraction view of current sates so that it can be interpreted by subsector organizations of various types, structures, and sizes.
- ➢ Benchmarking your organization and compare it to the subsector's

- Establish and maintain plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.
- Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.
- Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.

## OUR SECURITY INTELLIGENCE SERVICES INCLUDES

- 24 x 7 x 365 security monitoring and analysis.
- Detect & mitigate against any reconnaissance process, credential theft, and lateral movement.
- User Behavior Analytica
- Incident management.
- Platform management.
- Custom data source integration and custom parser development.
- Vulnerability Management.
- Profiling of security controls.
- ADSIC or FEDNet Reporting.

**DISCLAIMER**

THIS DOCUMENT CONTAINS INFORMATION THAT IS PROPRIETARY TO CYBER GATE DEFENSE LLC. NO PART OF THIS PREREQUISITE MAY BE DUPLICATED OR USED FOR TECHNICAL OR COMMERCIAL PURPOSES WITHOUT THE PRIOR CONSENT OF CYBER GATE DEFENSE LLC.

**TELEPHONE & FAX**
+971 (0) 2 6655 855
+971 (0) 2 6712 211

**ADDRESS**
Al Bostan Tower (Office 103), Abu Dhabi,
UAE. PO BOX 43123

**WEB**
soc@cybergate.tec
www.cybergate.tec