Whitepaper

# Asset Classification

WE HAVE THE IN-HOUSE DEPTH AND BREADTH 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.

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

## 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 CyberGate 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 Cyber 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.

## Table of Contents

## What’s Asset Classification?

Do you know what and where critical assets in your organization are? Do you know their value? What about the impact of their disclosure, corruption or loss? Organizations depend on critical assets to operate and therefore require having a distinct view of assets throughout its lifecycle.

Asset classification is the process for determining the critical assets and the required control to protect it according to its sensitivity. The process can be applied to any asset that has value, including business processes and environments.

Since not all assets have the same value or importance, different classification level may apply to different assets. A classification schema should be established and applied throughout the organization based on the confidentiality of each asset.

## Why Asset Classification?

Business and financial tasks are not exposed to unacceptable risk; why Should IT be? Organizations are keen on assessing risks when it comes to financial and or strategic task in order to maximize gain, enhance market share and reduce risk. Despite these tasks are highly dependent on technology, yet IT risks are commonly ignored, jeopardizing accuracy, integrity, confidentiality and availability.

Unprotected tools used to carryout business and financial tasks compromise the tasks performed using it. We understand that assets are as weak as their feeble links. Therefore, IT infrastructure must have the same level of confidence that business and financial tasks usually receive.

A strategic risk assessment not only allow business to meet its objectives and grasp opportunities but also enable organizations to add value to their core product and service, empowering business partners, protecting relationships and leveraging trust.

Accurately classifying assets is an analogy to creating a firm foundation for a high-rise building - understanding your assets and their value results in assigning the right control necessary to prevent them from being exposed to risk.

Asset classification is an important first step in the process of risk assessment. However, we understand the challenges of successfully preforming this task; business owners commonly believe that their assets are the most important but this view may not be shared with C level members.

Creating the right balance between the different assets across the organization is a key for effective protection. This will require a good understanding of business goals and objectives – designing the link between assets and crucial business activities.

A purely compliance-driven assessment may expose organizations to threats that are not yet addressed by the regulation. For example, ISO 27001 doesn't cover topics similar to cloud security and cybercrimes. Designing the right assets classification system will not only help identify organization risk but will also confirm to regulations. As there are many different standards and regulations it will be costly to address each separately. Adopting the right architectural design will provide sufficient flexibility to incorporate choice and change of policy, standards, practices, or legislation.

## Our Approach

When it comes to classifying assets, it is important to keep it simple, distinct and intuitive. We follow a simplified standard which has been carefully chosen with room for customization.

The recommended classification method is based on three-level approach. Each level attracts a baseline set of security controls providing appropriate protection against typical threats. Business Impact Level scale will also be customized to range from 0 (no impact) to 6 (extreme impact).

We start with accurately identify and model organizational assets and correlating between asset classification and BIL (Business Impact Level).

The purpose of this exercise is to quickly relate different sets of assets including both logical and physical. This provides the necessary constructs to uniquely identify assets based on known attributes. The model itself provides a view of the organization and how technology supports business functions. In doing this we will never lose sight of your organization's goals, objectives, success factors and targets, ensuring that the security strategy is properly supported, enhanced and protected.

Focusing on priorities "business critical" and "mission critical" risks using language, that is understood by business managers for direct involvement in the process.

We will not replace ITIL or ISO 27001 or NIST but rather enable their deployment effectively and integrate it into the corporate specific needs. We follow a structured methodology to make the process consistent throughout the organization. Ensuring that it is effective, easy to conduct, and produce a clear picture of key information risks with a simplified process on how to handle conflicting classifications.

## Deliverable

- A customized handling process driven form requirements for each level of classification and at each stage of the information lifecycle; creation, processing, storing, archiving and deletion.
- We will provide business impact statements for various sectors following a common set of standards that lead to a consistent approach to business impact assessment.
- Asset classification policy to ensure that individuals who have a legitimate right to access an asset can do so, whilst also ensuring that assets are protected from those who have no right to access them. Our offering will include a roadmap for integrating all requirements.
- BIL (Business Impact Level) defining the Business Impact Level for Assets.

- Identifying and valuing assets
- Applying suitable metrics
- Ranking the risks in relative priority order
- Providing a basis for risk management decisions
- Identifying where additional controls are required
- Process of how to handle conflicting classifications

## What is required to get it right?

- Holistic understanding of business and technical goals and environment
- Broad technical knowledge – including current trends
- Broad methodology knowledge
- Analysis of requirements and problems
- Innovation
- Leadership
- Stakeholder management
- Communication and soft skills
- Awareness of project management, commercial and issues.

## 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.tech
www.cybergate.tech