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 Cyber Gate 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.

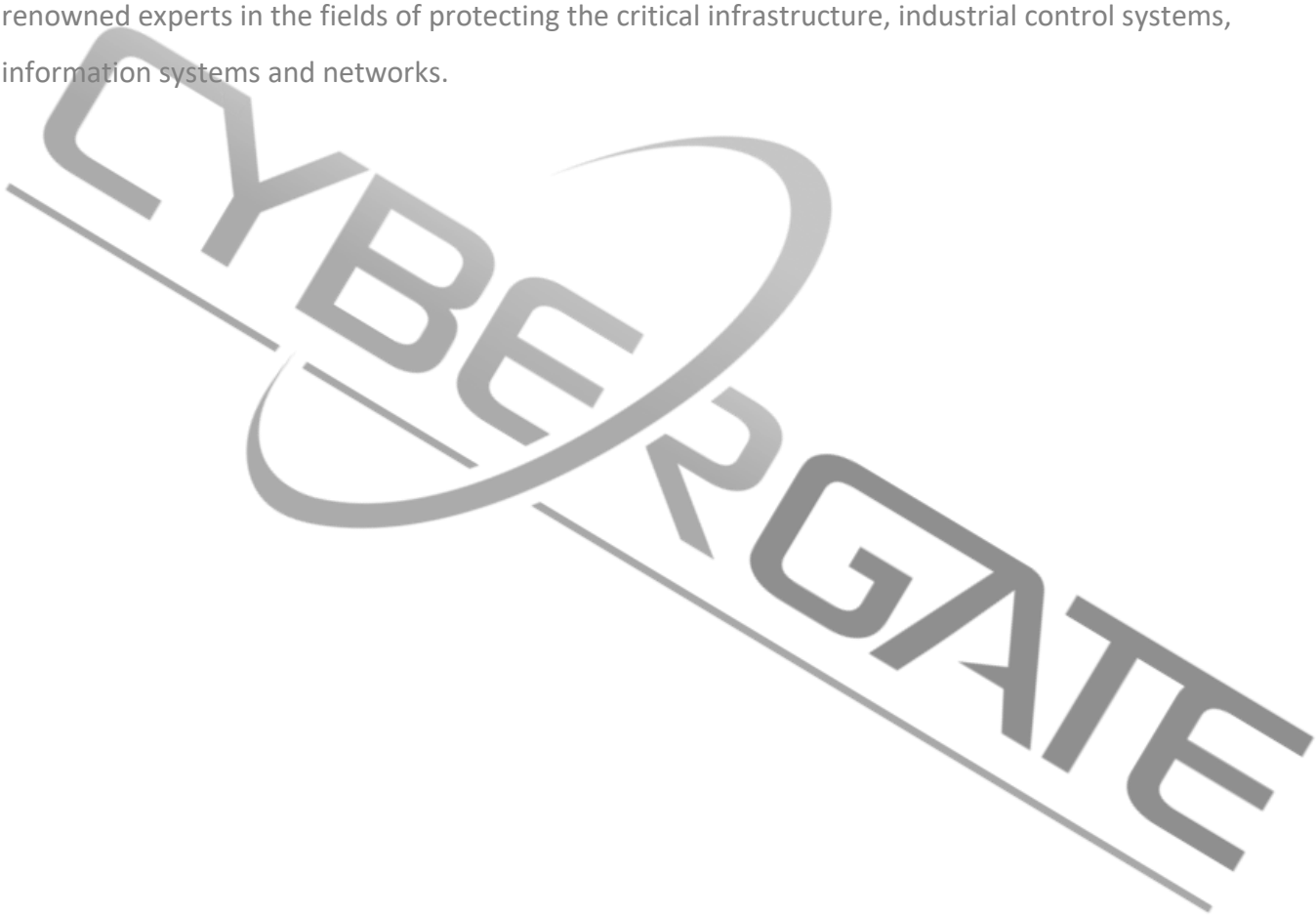

Table of Contents

What is Security Requirement?

Security requirement offers a method to capture and align security needs with business objectives. The process is intended to prioritize important requirements and avoid unnecessary cost associated with the Could Have requirements. It's a formal method for inspecting a security design and confirms it meets the requirement, measuring progress and realization of its benefits. It may be a condition or a statement of desires for a security capability required by stakeholders or to achieve an objective. Stakeholders will be able to know what security solution will be offered; clearly unambiguously and the scope of work can be defined.

Why Security Requirement?

Stakeholders will be given the opportunity to voice their needs and have it formally documented. A clear recorded security requirement is more effective because:

- Unambiguous. Eliminating false interpretation of requirement.
- Priority level is practically set. Favoring urgent requirements.
- Linked to a business objective. Validating value to the organization.
- Assigned Owner. Associate requirements with sponsors.
- Linked to other requirements. Eliminate duplication.
- Formal acceptance based on some predefined acceptance criteria. Avoid unexpected surprises.
- Functional category is clearly defined. Developing fit to purpose solution.

When utilizing the above features, an informative decision can be reached on whether a security requirement is necessary to implement. Selected security requirement can be formally accepted based on a predefined acceptance criteria and can be traced to a business objective.

Without a formal process governing requirements, organization risk is unlikely to be mitigated.

Security Requirement challenges?

Stakeholders who have a direct association with requirements such as users, developers, project sponsors, customers, security professionals, project managers and testers collaborate through a predefined security requirement process. However, as a consequence of considering a range of different perspectives there will inevitably be conflicts between different stakeholder views, and hence, a key part of security requirements is the resolution of such conflicts. The well planned security requirement should ultimately streamline the acceptance process.

Some of the other challenges:

- Ambiguous requirement is commonly seen when formal security requirement is absence leading to an ineffective control in managing interpretation of security requirements.
- Defining a good security requirement does not only mean an understanding of assets and their values, it is equally important to evaluate assets at different stages of their lifecycle; creation, processing, storing, archiving and deletion.
- Choosing the right security requirement, develop it on time within budget using available resources requires a specialized skills. It's cost effective to acquire professional services and have it correctly developed.

Our Approach

Our endeavor is to gain a good understanding of the organization context and business objectives. We then align security requirement to business objectives. Understanding the needs and expectations of interested parties leads to a solution that is fit to purpose.

Establishing a clear plan for requirements management and communication at the enterprise level is essential to support solution acceptance, assessment and validation.

Since security requirements can be captured in different ways, we therefore offer a set of various elicitation methods including: interviewing, workshop, questionnaire, brainstorming, observational, requirement reuse, documentation studies, laddering, repertory grid, scenarios, prototyping, and contextual inquiry. Each of these methods has its own engagement procedure and process.

We associate each individual requirement with an acceptance criteria insuring that security solutions logically map to requirements.

The increasing amount of security requirements can be overwhelming; we assign a priority level to each requirement based on the MoSCoW model. MoSCoW has four different rating; Most have, Should have, Could have, and Won't have. Each level has a different priority level ranging from highest to lowest respectively and the method is used to prioritize security requirement.

Security requirements undergo a classification process to determine whether it is functional or non-functional. Most security requirement fall in the non-functional category but in some cases; security feature needs to be developed and hence will be classified as functional.

Deliverable

Security requirements are captured and linked to business objective and assigned an owner. A complete set of a comprehensive and unambiguous security requirements documented in a catalogue specifically tailored to your organization will be provided upon completion of the project. Each security requirement will be given a priority level, classified whether it is a functional or non-functional any linked to other associated requirement in the catalogue.

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.

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