Cyber Security Professional Services

The impacts of a cyber-attack on a company's business are various and can cause considerable damages. Thefts of information can lead both to a financial loss and to legal consequences deriving from the fraudulent use of stolen data.
Financial or corporate information and even money can be subtracted during a cyber-attack. Fines and regulatory sanctions can be the result of data loss especially when companies fail to implement the appropriate security measures. Costs can also be generated by the need to repair the affected digital infrastructures – datacentres, single devices or networks. Moreover, data breaches can lead to a shift in sentiment for companies or institutions.
These situations cause reputation damages that can bring not only to a loss of customers but also of suppliers.

LEONARDO CYBER SECURITY CONSULTING

Leonardo's Cyber Security Consulting team support our customers to deal with the design, implementation and management of a Security Governance Framework to increase cyber resilience in both ICT sector and OT systems. Highly skilled professionals support public administrations, critical national infrastructures and enterprises to:

- define the processes to manage the organization's security;
- define and implement the adequate security measures to protect networks, data and infrastructures;
- define and implement Information Security Management System to comply with laws and regulations

Leonardo's cyber security professional services address two areas, closely integrated, which include activities both to support the implementation of Customers' Security Governance and services aimed at increasing the Cyber Resilience of companies and organizations. Our offer includes consulting and analysis activities provided by professionals often using tools and specific products to supports their tasks.
According to the specific customers' needs, the services can be integrated into offer bundles to provide a comprehensive and integrated approach to Security Governance and Cyber Resilience topics or can be provided individually to investigate specific aspects.

SECURITY GOVERNANCE

The Security Governance services aim at designing and operating a Security Governance Framework to manage organization's cyber security. The Security Governance Framework guarantees the adoption of a security level in line with the policies, customer's security strategies and business objectives as well as with current laws and regulations.

LEONARDO

Security strategies and objectives are defined, the most appropriate organizational model is determined, the necessary processes and services specified and the IT tools to support processes and services are identified. These services also provide support in risk analysis and management process, applying the principles and concepts of leading methodologies such as IRAM (Integrated Risk Assessment Method), Ebios and ISO 27005.
Security Governance includes also assessment, audit and gap analysis for compliance with standards and regulations related to information, privacy or physical security.

CYBER RESILIENCE

The adoption of a cyber resilience strategy helps organizations to protect their technological context against cyber risks and to reduce the severity of cyber-attacks.
Cyber Resilience services provide the analysis of networks, systems and applications in the customer's operative environment to detect vulnerabilities, to identify risks and, consequently, to define the needed remediation actions. Platforms and processes are analysed starting from the customers' needs and requirements or from the detection of the attack surfaces more exposed to cyber risks.

Cyber security requirements are also identified according to regulations and standards specifically designed to protect and defend information and IT infrastructures or to establish security policies and assign responsibilities to minimize the risks (DoDI 8500.01, 5200.44, ISA/IEC 62443, Common Criteria, ...).

Cyber resilience services can be provided during the definition of the customer's cyber security and cyber resilience strategy, during the design of secure by design systems and applications, periodically or following particular events (introduction of technological innovations). Such activities include:

- The "modelling of threats", through the modelling of industrial platforms or complex systems, physical and logical components, modules or subsystems. Threats and new security requirements are identified to address the eventual design or re-design of platforms and systems, the execution of targeted tests and penetration tests and the upgrade of software and firmware according to the Security Software Development Life Cycle (SSDLC) methodology.
- The "vulnerability assessment", based on the definition of the intervention domain and objectives (preparation), the collection of critical information (collection), the analysis and prioritization of vulnerabilities (analysis) and the generation of recommendations (distribution).
- The "penetration test" aimed at evaluating the security status of a system or a network. This service allows to verify and consolidate the vulnerabilities identified during the vulnerability assessment and to find new ones, through ethical hacking techniques.
- The definition of additional security requirements and of mechanisms or solutions to be integrated into the customers' networks, systems and applications to enhance cyber security and to introduce cyber resilience capabilities

An important application context of these services is represented by the OT networks in which Leonardo has developed specific competences for the protection of SCADA systems.

LEONARDO SECURITY EVALUATION FACILITY

A Security Evaluation Laboratory (LVS) is also available to evaluate and certify the security of systems and products pertaining to the information technology sector. The laboratory is qualified by the Italian Information Security Certification Body (OCSI), and operates since 1997. It was merged in Leonardo in 2017 and acts as a Security Assessment Laboratory, a global consultant for physical, organisational and ICT security and as a consultant in Italy for military certifications consistently with the National Security directives.

For more information please email:
ict-cyber@leonardocompany.com

Leonardo S.p.a.
Via Laurentina, 760 - 00143 Rome - Italy
Tel. +39 06 50271
Fax +39 06 5051140

leonardocompany.com

SIS MM09028 09-19

LEONARDO