



SPARTAN
INFOTECH

IT
Security
Offering

March 31

2008

Spartan Infotech Co. WLL



Company Profile

Spartan Infotech Co. WLL is part of the Mohamed Ahmadi group of companies.

The group has over 3 decades of experience in the Middle East and a multi-million Dinar (1USD=0.378BHD) turnover spanning operations such as Trading and Contracting, Cleaning and Maintenance, Cargo Forwarding, Ship Repair, Interior Design and ICT.

Spartan Infotech is led by Ashok Kumar, with over 15 years experience handling the business of reputed brands (Samsung, Fujitsu-Siemens, Emerson, Asco, Seagate Software) as General Manager at the respective country distributors. His last assignment was at an ICT multi-national as Director, Strategy and Corporate Development.

Spartan Infotech is a technology venture and comprises of discrete divisions that run as profit centers under experienced Division Managers. Division Managers are aided by qualified Practice Heads that are abreast of the latest developments in the respective areas.

Spartan Infotech has established strategic alliances with reputed principals in areas such as Enterprise Asset Management, Process Control, Customer Relationship Management, Enterprise Resource Planning, IT Security and implementation of standards based frameworks for IT governance. Other Lines of Business include Consultancy, Implementation and Support of ICT Networks.

Spartan Infotech Co. WLL

2nd Floor, No. 668, Al Hassan Building, Diplomatic Area 317, Manama, Kingdom of Bahrain
Email: info@spartaninfotech.com, Website: www.spartaninfotech.com

DRIVEN BY INNOVATION

IT Security

IT Security is the protection of data, resources and information against disasters, mistakes and manipulation so that the likelihood and impact of security incidents is minimized.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked." - Former White House cybersecurity adviser, Richard Clarke

Components of IT Security

IT security is comprised of:

1. **Confidentiality:** Assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner appropriate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc.
2. **Integrity:** Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term 'integrity' is used frequently when considering information security as it represents one of the primary indicators of information security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon.
3. **Availability:** Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
4. **Accountability:** Someone is personally accountable and responsible for the protection of an asset or set of assets. The emphasis here is on the 'someone' and the 'personally accountable'. Often this does not work in the organisational setup but it still should be the goal.
5. **Auditability:** This component has two parts, firstly that any position that a system is found in should be able to be backtracked to determine how it got into that state and secondly, that an ongoing process of management review or audit should be undertaken to ensure that the systems meet all documented requirements.

(source: ISO 27001)

Benefits of IT Security Management

1. Ensures the safety of valuable IT assets
2. Helps to minimize waste and ensure that the resources expended on security contribute to optimum production and output
3. Protects resources from damage, loss or waste
4. Takes all necessary precautions to contain and limit threats from having a negative impact on essential information systems

Spartan Expertise

Whether you manage a small business or a large enterprise, **IT security** is one area where you cannot afford to miss a single detail.

All it takes is one missing element in your **IT security** plan to leave your business open to network attacks and operational disasters - with possible financial and legal consequences. To make matters worse, new regulations and standards are being introduced frequently.

In order to ensure your **IT security** is up-to-date and compliant with the latest ISO 27000, HIPAA and Sarbanes-Oxley standards, Spartan Infotech Co. WLL has teamed with SecureITLab to bring you top notch consultants that will conduct periodic review and assessment of your infrastructure so that you can be at ease with this critical aspect of your business.

Our domain expertise extends to the following processes:

1. Security Assessments and Audits:
 - a. **Penetration tests:** A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, known as a hacker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. [wikipedia]
 - b. Network audits

Spartan Infotech Co. WLL

2nd Floor, No. 668, Al Hassan Building, Diplomatic Area 317, Manama, Kingdom of Bahrain
Email: info@spartaninfotech.com, Website: www.spartaninfotech.com



- c. **Vulnerability Assessments:** Vulnerability analysis is the process of identifying, quantifying, and prioritizing (or ranking) the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability assessment can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.
 - d. Application security audits.
 2. Information Risk Management: Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.
 - a. Implementation of standards-based control frameworks such as ISO 27001, ISO 20000, BS 25999
 3. Security Implementation
 - a. designing secure network architectures, implementing the right security solutions and developing proper processes for these.
 4. Computer Forensics and Incident Response
 5. Business Continuity Management
 6. Enterprise Risk Management
 7. PCI Compliance
 8. **Security Incident and Event Management:** Security incident management is an administrative function of managing and protecting assets, networks and information systems.
 9. **Code review:** Code review is systematic examination of computer source code intended to find and fix mistakes overlooked in the initial development phase. It also checks for malicious code that may be written into the source for whatever reason.
 10. Information Security Trainings

Key differentiators

1. Strong focus on research and innovation
2. Internal employee focus with trainings and certifications programs: CISSP, CISA, CEH and Encase Certifications
3. Internal information security compliance: SecureITLab is one of the very few ISO 27001 certified security companies globally
4. Strong global delivery model: with numerous overseas projects successfully completed, we have a robust onsite-offsite delivery model that ensures we deliver tremendous value on all our assignments.

For any enquiries, please send us a mail at marketing@spartaninfotech.com

ⁱ References: Wikipedia, ISO 27001, Communications Security Establishment