Risk Management Services

Information Security Consulting Services

The dependency on modern information systems to perform critical and core business functions is increasing everyday. Such information systems do not work independently, rather they interconnect with other systems, some may be in-house hosted and others could be managed by a system service provider. Thus, assuring that customer or corporate information security is becoming a main concern for the Chief Information Officers, Corporate Planners and/or Chief Security officers. The concern on information security assurance rises from the availability of third party software, faster software development life cycle, number of users accessing the systems, exposure to the internet and virus and malicious software. Lack of information security assurance level results in what is called "information risk" and requires a Risk Management methodology to identify such risks and manage them.

Risk Management includes various processes: risk assessment, mitigation, evaluation. Risk Assessment is a core process in risk management and it aims at providing decision-makers with information needed to understand factors that can negatively influence operations and outcomes in order to make informed judgments concerning the extent of actions needed to reduce risks. It entails identifying and analyzing threats and vulnerabilities of an information system, and determining potential adverse effects that would impact the organization in case of a compromise. Risk Mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended by the risk assessment process. Risk Evaluation aims at evaluating process and security measurement keys for implementing a successful risk management program.

The end result will allow the Chief Information Officer and/or Corporate Planners to balance the operation and cost of protective measures to protect the organization's IT environment and support its missions and business objectives

We at VERSOS realize those risk challenges, and offer a comprehensive suite of services to assess such risks and provide mitigation plans and recommendations. VERSOS Risk Assessment/ Management suite of services encompasses:

- **Vulnerability Assessment**
- **Penetration Testing**
- **Application, Code Review and Security Assessment**
- **Business Impact Analysis Report**
- **Development of Risk Mitigation Plan**
- **War-driving and Wireless Penetration Testing**

Versos
Providing what matters...

Web: www.versos.com.sa
E-mail: sales@versos.com.sa
Tel: +966 1 473 5932
Fax: +966 1 473 5931

Suite # 203 - Al-Umam Commercial Center - Siteen Street
P.O.Box 255390, Riyadh 11353,
Kingdom of Saudi Arabia

Risk Assessment:
Vulnerability Assessment

"Phishing kits are beginning to be used on a widespread basis."

"a look at the three most widely used phishing tool-kits reveals that they alone were responsible for 42 per-cent of all phishing attacks detected in the first half of 2007"

symantec.

Symantec Internet Security

SECURE OPERATION

Virus attacks continue to be the source of the greatest financial losses. Unauthor-ized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial

CSI COMPUTER SECURITY INSTITUTE

Vulnerability Assessment is a security exercise that aid business owners and security professionals in identifying security liabilities within networks, applications and systems. Vulnerabilities Scanning aims at findings threats, flaws and/or weaknesses in system security procedures, design, implementation or internal controls that could be compromised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the systems security policy.

VERSOS has adopted a Vulnerability Assessment methodology that is based on international standards. VERSOS methodology encompasses: Discovery, Exploration, Analysis and Reporting phases.

Our consulting team uses many tools and applications to aid in the discovery of technical information such as: finding live hosts, porting and service scanning, perimeter network mapping (routers, firewalls), identifying critical ports/services, operating system fingerprinting and service fingerprinting.

VERSOS consulting team will also performs several activities to detect exploitable points such as design weaknesses, configuration and implementation flaws, etc. These activities include:

- Identifying vulnerable services using system and service banners.
- Performing vulnerability scans to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as NIST, SecurityFocus, CVE, CERT advisories or any other best practice source.
- Performing false positive and false negative verifications (e.g. by correlating vulnerabilities with each other and with previously acquired information).
- Enumerating discovered vulnerabilities.
- Estimating probable impact (classify vulnerabilities found).
- Identifying attack paths and scenarios for exploitation.

After completing Vulnerabilities Assessment, a workshop is held with the client, to review and validate the findings, to highlight any issues that may require immediate attention, and to confirm the action plan for next level of testing.

VERSOS comprehensive offering include Vulnerability Assessment and Mitigation to ensure that your IT operations and security posture is up-to-date and secure.

Versos
Providing what matters...

Web: www.versos.com.sa
E-mail: sales@versos.com.sa
Tel: +966 1 473 5932
Fax: +966 1 473 5931

Suite # 203 - Al-Umam Commercial Center - Siteen Street
P.O.Box 255390, Riyadh 11353,
Kingdom of Saudi Arabia

Risk Assessment:
Penetration Testing

***"Penetration testing can actually be an excellent approach to a security audit, especially at the boundaries of networks, where acquisitions may have introduced network weaknesses that have not yet been identified."*— CERT, www.cert.org**

"But since attackers have moved from vulnerability scanning to fairly targeted penetration testing, companies now need to carry out penetration testing before the attackers do" — Joe

SECURE NETWORK

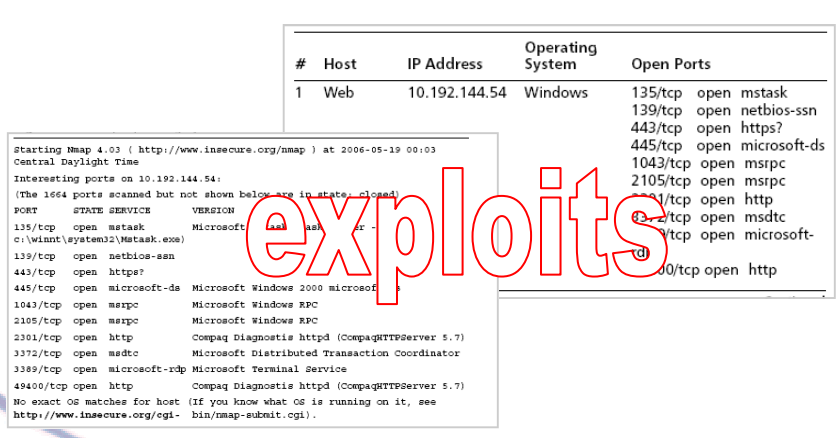
Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial

CSI COMPUTER SECURITY INSTITUTE

The importance to secure information is high, specially if vulnerabilities are reported during a vulnerability assessment exercise. The existence of specific vulnerability may lead to a security breach thus exposing information resources to illegal or accidental access. A Penetration Test is the process of evaluating the security posture of a computer system, network, or application (assets). The process involves analyzing assets for any weaknesses, configuration flaws, or vulnerabilities to determine whether a certain system can be hacked or exposed.

VERSOS consulting team has Certified Ethical Hackers (CEH) who possess the right non-destructive tools, experience and methodology to explore, exploit and evaluate the security posture of your network and servers. VERSOS consulting team can perform black and white box penetration testing and provide feedback in a timely manner. Our approach is based on international best practices and Open Source Security Testing Methodology Manual OSSTMM

VERSOS value added services provide customers with recommendations, additional controls and proposed network design to resolve exploits and thus increase the level of security.



Versos
Providing what matters...

Web: www.versos.com.sa
E-mail: sales@versos.com.sa
Tel: +966 1 473 5932
Fax: +966 1 473 5931

Suite # 203 - Al-Umam Commercial Center - Siteen Street
P.O.Box 255390, Riyadh 11353,
Kingdom of Saudi Arabia

Risk Assessment: Application Security Assessment

The gaping security loop-hole in Web applications is being exploited by hackers worldwide. According to a survey by the Gartner Group, almost three-fourths of all Internet assaults are targeted at Web applica-tions—Source: http:// www.windowsecurity.com

SECURE APPLICATION

Virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to lap-tops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74 percent of financial losses.

Software applications imposes various types of challenges and risks. Therefore, proper controls should be exercised for the protection of software and the infor-mation that is processed by the software. Assuring the security of any application within the organization is of equal importance to securing a network device, server or firewall. VERSOS realizes and understands those risks and has devel-oped a comprehensive methodology to assess application security and provide sufficient assurance that information processed or stored by these application is secure.

A combination of automated security assessment tools and human-initiated are used to perform a comprehensive Application Security Assessment. VERSOS con-sultants possess an extensive knowledge in software development lifecycle, appli-cation testing, using automated tools and designing testing scripts to ensure that your applications are secure. VERSOS consultants base their findings and tests on Open Web Application Security Project (OWASP) which has identified top 10 ap-plication vulnerabilities and they are

A1– Cross-Site Scripting (XXS)	A6– Information Leakage and Improper Error handling
A2– Injection Flaws	A7– Broken Authentication and Session Man-agement
A3– Malicious File Execution	A8– Insecure Cryptography Storage
A4– Insecure Direct Object Reference	A9– Insecure Communication
A5– Cross Site Request Forgery (CSRF)	A10– Failure to restrict URL Access

VERSOS consultants designs various test scenarios in order to achieve a better understanding of the application security posture including

Account Harvesting	Token/Cookie Analysis
Access Control Testing	Session Management
SQL Injections	Buffer Overflow
Input Validation	Cryptography Implementation Review
Code/content Injection	Logging Practice Review

Often, a combination of these assessment techniques are used in conjunction to gain more comprehensive application assessment of the overall application secu-rity posture. Shall you require more technical details please contact us as below.

Versos
Providing what matters...

Web: www.versos.com.sa
E-mail: sales@versos.com.sa
Tel: +966 1 473 5932
Fax: +966 1 473 5931

Suite # 203 - Al-Umam Commercial Center - Siteen Street
P.O.Box 255390, Riyadh 11353,
Kingdom of Saudi Arabia