

# xDEFENDERS, INC.

INFORMATION SECURITY SOLUTIONS

**Security Consulting** xDefenders helps organizations comply with Information Security Regulations, Privacy Laws, and Best Security Practices to protect their applications, databases, systems, and networks using our personalized, professional service.

- Best Practices and Best Protections
- Secure Routing, Switching & Firewall Configurations
- Secure Remote Access and Authentication
- Security Architecture Review
- IPS and IDS Optimization w/ Escalation
- High-Availability Configurations

## Credentials

- Expertise with ISO, HIPAA, PCI, Homeland Security, NYS Security Policy and Standards
- GLBA, NCUA, FFIEC —Financial Industry Security Rules and Regulations
- CISSP —Certified Information Security System Professionals
- CISA —Certified Information Systems Auditor
- CERT —Computer Emergency Response Center
- CIS —Center for Internet Security benchmarks
- Security Operations Center —Tier 4 Class, SAS 70 Data Center



**History** Since 2003, xDefenders has focused exclusively on Information Security for business. We have enterprise-class experience with systems, networking, web application development, and proven methodologies. xDefenders has a large client base across the USA. The company was acquired by Synergy Global Solutions early in 2007. Synergy, founded in 1971, has over 200 employees.

**Professional Services** xDefenders is an experienced team of Certified Information System Security Professionals (CISSP) focused on helping organizations protect the confidentiality, integrity, and availability of their information assets. We address the important elements that help mitigate risk and must be addressed in this process: people, policies, and procedures.

## Vulnerability Assessments

These technical risk assessment services are based on accepted, industry-wide standards and methods, which include planned and unplanned “penetration” tests upon your network, systems and applications to determine their level of *vulnerability*. This will help you determine your risk at each level of the business. Our testing plan is comprehensive:

\* *Internet, External Networks*   \* *Social Engineering*   \* *Modems, Wireless*   \* *Web Applications, Databases*

xDefenders will classify your vulnerabilities – open ports, down-level operating systems and suspect applications - as *Urgent-Critical-High-Medium-Low Risk*. We do not exploit found vulnerabilities. Our CISSP’s will produce Management and Technical Reports and review them with you during an interactive session. Periodic and ad-hoc testing is recommended and our Subscription Service is offered monthly or quarterly. The **SysDefender** Test Appliance is our portable tool. It is updated in real-time with known vulnerabilities and contains a complete set of tests and methods to assess vulnerabilities. xDefenders will securely ship this appliance anywhere in the USA, to keep costs low.

## I/T Security Audit

Based on ISO, FISAP and other Regulatory Standards, xDefenders works with clients to interview employees, I/T staff and management to determine if published security policies are being followed. We compare policy with procedures and note where there are "gaps". A detailed checklist is completed and a report is written and reviewed with the client. An audit will review the following areas:

### ♦ Web Application Security

We will audit your key web applications using OWASP standards and provide you with a report that will detail all remediation needed to secure the applications. We use a number of the industry's best tools. These tools can be run remotely and provide information on a number of known exploits including:

- Cookie poisoning - Identity Theft
- Hidden field manipulation - eShoplifting
- Parameter tampering - Fraud
- Buffer overflow - Closure of business
- Cross-Site scripting - Hijacking/Breach of trust
- Manipulation of SQL statements
- Backdoor and Debug Options - Trespassing
- Forceful browsing - breaking and Entering
- Stealth commanding - Concealed Weapons
- 3rd party manipulation - Debilitating a site
- Known vulnerabilities - Taking control of a site

### ♦ Database Access and Security Controls

Many applications that reside on top of Oracle, Sybase, DB2, MS/SQL or MySQL rely on the security attributes of the database to secure, control and backup the data. Understanding this concept and Data Base Administrator (DBA) processes and tools, is essential to auditing a database and the applications that utilize it. We look at the relationship between application and database security.

- Log-On Procedures
- Password administration and management
- User Identification, Authentication, Admin.
- Use of system utilities
- Links to applications, operating systems
- Backup and storage security procedures
- Security of DBA tools and software
- Evaluation of stored procedures

### ♦ Housekeeping

- Management of Logs
- Back-up Procedures
- Fault Logging
- Problem Reporting and Administration

### ♦ Operating System Access Control

- Password Administration and Management
- User Identification, Authentication, Admin.
- Use of System Utilities
- Terminal Time-out
- Limitation of Connection Time
- Terminal Log-On Procedures
- Peripheral Administration

### ♦ Security of System Files and Servers

- Control of operational software
- Protection of system data and files
- Access control to program source library
- Connectivity and Interconnected network
- Network Access
- Trust relationships
- Server Logical Security
- Penetration detection
- Violation investigation and monitoring
- Virus Protection
- Remote access facilities and VPN controls
- Authentication mechanisms

### Security Policy Development & Review

A set of security policies is a reflection of the culture of the organization. It needs to be clearly articulated and communicated to employees and business partners. We can provide and/or comment on, well-constructed and publicized security policies.

### Employee Awareness Training

Most organizations are vulnerable to Social Engineering attempts to gain vital knowledge, which can lead to a compromise. xDefenders offers Security Training to help clients increase awareness, reduce their risk of compromise.

### Business Impact Analysis, Continuity Planning

Business Continuity Planning (BCP) is a collection of management processes designed to provide organizational persistence during and following a business disaster. This project begins with the data collection and interview process called - Business Impact Analysis (BIA).

### Risk Assessment

xDefenders can help assess the level of security you need to design into your applications, systems and networks by following a proven evaluation model. This Information Risk Management Plan compares and considers key information components and helps you assign a security service for data or program segment to be secured, and the costs associated with the desired security service. The Plan will provide for the adequate protection of all proprietary, confidential, and privileged information assets valuable to your company, from all threats, whether internal or external, deliberate or accidental.