

## Technology, Security & Compliance

Capsicum consultants have conducted numerous investigations in response to computer hacking, intellectual property theft, employment issues, and other security concerns. We are well aware of the many vulnerabilities exploited by intruders. Utilizing our knowledge of regulatory guidelines and information security best practices, we put together solutions that will diminish your risks.

### Information Security Assessments

Capsicum's Information Security Assessments focus on your organization's electronic assets. We employ a "top-down" approach to evaluating the security of your information, beginning with policies and procedures.

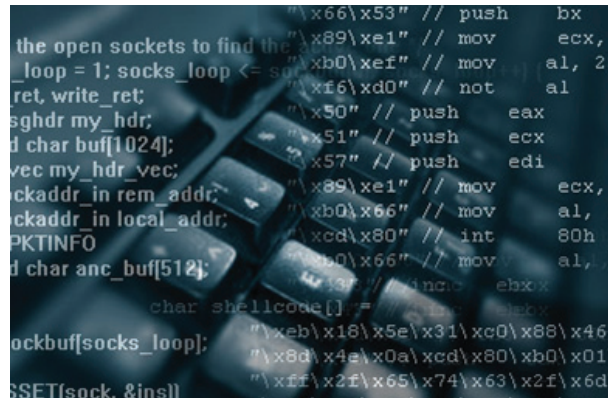
The next phase of our assessment involves verification that the policies and procedures you have in place are actually being followed and enforced. Through interviews and both, automated and manual checks, we audit many aspects of information security including:

- Access Control
- Communications and Network Security
- Application, Web, and Database Security
- Physical Premises Security
- Personnel Security and Awareness
- Operations Management
- Business Continuity and Disaster Recovery Readiness
- Regulatory Compliance
- Incident Response Readiness
- Areas of Unique Concern

In our final phase, Capsicum will identify your security vulnerabilities and the risks associated with them. We will provide you with an expert report, tailored to your organization, which will identify the issues and rate the associated risk level.

### Network and Application Security Evaluation

The overall level of Information Security is only as strong as its weakest link. Today, organizations are faced with constant virus and malware outbreaks, intrusions by hackers, and threats from trusted internal users.



Capsicum is able to put itself into the mind set of a potential intruder to expose the gaps in your information security. We are able to offer the following services:

- **Vulnerability Scanning** – Capsicum identifies vulnerabilities that an attacker can exploit.
- **Manual Vulnerability Analysis** – Capsicum confirms vulnerabilities identified by automated scans decreasing false positives and saving time required to address these security issues.
- **Penetration Testing** – We simulate a potential attacker and attempt to penetrate your defenses to gain access to your information.
- **Application and Database Review** – We review your application and database security to minimize the risk of an attacker gaining access to sensitive information.

Capsicum can test External and Internal Security, Border Security, Wireless Security, Server Configuration, Endpoint Security, Network and Communications Security, and other areas as required.

## Technology, Security & Compliance

### Incident Response

Even the most secure networks can be breached. If a breach occurs, proper procedures must be followed to preserve volatile evidence. Capsicum consultants are experienced in data collection and analysis of computer breaches. We offer the following services:

- **Data collection** – Capsicum will capture volatile and non-volatile data.
- **Forensic Analysis** – Our experts will analyze the acquired evidence to identify the attack vector and the intruder.
- **Legal Support** – Capsicum will work with your legal team or law enforcement to draft subpoenas and other documents to establish the identity of the intruder.

If a security breach does occur, it is vital that an experienced team is engaged to limit its impact and identify its source.

### Regulatory Compliance Reviews

Capsicum has developed a simple yet comprehensive program to provide regulatory compliance for information technology environments. Capsicum offers consulting services related to HIPAA (Health Insurance Privacy and Accountability Act), COPPA (Children's Online Privacy Protection Act), SOX (Sarbanes-Oxley Act), GLB (Gramm-Leach-Bliley Act), Personal Data Privacy and Security Act, and other industry programs.

Our compliance program includes the following services:

- **Assess** – Review current policies, processes, organization and technology to develop preliminary findings and recommendations. Determine applicable regulations and develop a detailed analysis that will provide a "composite" view of the organization's requirements.

- **Plan** – Recommend actions, determine risks and benefits, develop estimates for remediation activities, and provide a summary of the financial impacts (annualized) and the potential return on these investments.
- **Design** – Develop the detailed tasks and technology architecture necessary to execute the compliance program.
- **Implement/Remediate** – Articulate and document processes (additions, deletions, and changes), with relevant controls isolated, and technology (hardware, software, network) that should be acquired, installed, and/or configured.
- **Monitor/Upgrade** – Evaluate, subsequent to a comprehensive or more targeted compliance effort, each element on a quarterly or semi-annual basis.
- **Compliance** – Capsicum helps the organization become compliant with relevant regulations, and "best practices." The benefit to the organization of this approach includes: (1) reduced costs, (2) use of broad industry knowledge, (3) coordination of compliance and technical aspects, (4) increased efficiency, (5) completion of work in shorter time, (6) reduced interference with the organization's activities, and (6) in many cases, use of information platforms that already exist.

Electronically stored data is critical to modern operations. Many organizations never recover from serious security incidents. Don't let a potential disaster threaten your place of work. Contact Capsicum today.