

VeriSign[®] Network Security Consulting



VERISIGN BLENDS UNMATCHED SECURITY EXPERTISE WITH
WORLD-CLASS PROGRAM MANAGEMENT TO PROVIDE A
COMPREHENSIVE LINE OF NETWORK CONSULTING SERVICES.



Using a business-driven approach, VeriSign's experts are skilled in the art of risk mitigation and provide the necessary balance between bulletproof protection and cost. With a singular focus and a requirement for 100 percent customer satisfaction, VeriSign separates its services into three areas:

- Security Assessments
- Security Programs
- Security Technology

VeriSign's consulting team includes one of the highest concentrations of credentialed experts in the industry. With an average of 10-years experience per consultant, VeriSign boasts expertise across the entire information security and privacy spectrum.



SECURITY ASSESSMENTS

VeriSign's Security Assessments ensure that each level of an organization's information infrastructure meets the specific customer's information security objectives. VeriSign uses its customer's internal policies, industry standards of good practice and applicable laws and regulations to create a focused gap analysis that identifies areas of high risk and recommended remediation efforts. VeriSign's assessment services range from enterprise-wide evaluations to individual program and code-reviews, including:

- Enterprise Security Assessment
- Network Architecture Assessment
- Network Vulnerability Assessment
- Application Vulnerability Assessment
- Application Code Review
- Wireless Security Assessment

Enterprise Security Assessment (ESA)

VeriSign's ESA service provides a detailed assessment of an organization based on the following five areas:

- Security policy and processes
- Security/privacy program management
- Technology infrastructure and security controls
- Security organization and governance
- Operational effectiveness

In-depth evaluation of these key areas enables VeriSign to describe an organization's overall security objectives and assess its current ability to support them. Keeping pace with the dynamic security threats facing an organization, ESA compares each area to the evolving vulnerabilities and business risks that are relevant to each specific customer. VeriSign identifies the strengths and weaknesses of its customers, and recommends practical measures to align a security program with their business objectives. ESA helps clients:

- Prioritize spending for the highest value and highest risk security and privacy efforts
- Track changes in their security program and provide a long-term perspective on its effectiveness
- Improve the accuracy of due diligence efforts during a merger, acquisition, or strategic partnership

Network Architecture Assessment

VeriSign's Network Architecture Assessment analyzes a customer's physical and logical network topology with a detailed examination of three critical areas:

- Network device configuration
- Management and monitoring capability
- Location and configuration of critical network services

The assessment results are compared with an organization's overall security objectives and a detailed report identifies network strengths, weaknesses, and recommendations for improvement.

Network Vulnerability Assessment

VeriSign's Network Vulnerability Assessment identifies network vulnerabilities using the most sophisticated techniques available. Mimicking a malicious intruder, VeriSign gathers network information, runs automated scanning tools, and uses extensive manual testing to discover network vulnerabilities.

VeriSign's external network vulnerability testing probes Internet points-of-presence for known security vulnerabilities; internal network vulnerability testing assesses network security from inside a DMZ or from within an organization. All testing uses strict controls with an emphasis on protecting each client's security and privacy.

Application Vulnerability Assessment

VeriSign's Application Vulnerability Assessment identifies security vulnerabilities by reviewing and probing an application's security controls. This "black box" security testing examines an application's run-time behavior using a variety of techniques customized for each application type. Examples of some Application Vulnerability Assessment tests include:

- Testing the ability to replay authentication data
- Looking for exposure of sensitive data on servers
- Attempting to exploit encryption algorithms
- Taking advantage of inadequate input validation controls

Tests are performed both from the perspective of a trusted user and as an anonymous user (without valid user credentials). A detailed findings report including a prioritized issues list and recommendations for remediation of discovered vulnerabilities is provided.

Application Code Review

Application Code Review is one of VeriSign's most in-depth security assessments. Starting with an application security architecture review, VeriSign analyzes the application's source code from the perspective of a developer looking for design flaws, programming flaws and the use of vulnerable functions or programming constructs. Any one of these weaknesses can be buried in thousands or millions of lines of application code, and VeriSign performs the arduous task of finding these flaws. VeriSign then details its findings in a clear, concise and actionable report. Designed to precede the "black-box" testing done in an Application Vulnerability Assessment, this service is typically performed in the middle of an engineering cycle to more easily remedy architectural weaknesses.

Wireless Security Assessment

VeriSign's Wireless Security Assessment helps clients identify and mitigate risks and vulnerabilities associated with their wireless networks. This business-focused service includes the following elements:

- A review of the underlying requirements for wireless networks
- Review of the wireless network architecture, configurations and standards, as well as a detailed review of an organization's wireless deployment strategies, policies and procedures
- Identification of signal leakage and deployment of unauthorized access points in the enterprise, along with the identification of vulnerabilities in access points and wireless LAN clients
- Appropriate use of encryption technologies to minimize leakage of clear text information

VeriSign details findings in a report that offers a risk-level classification and impact analysis for deploying wireless LAN technology, including the development of "what-if" scenarios to assess the impact of a security compromise. VeriSign also includes recommendations to mitigate risks and vulnerabilities associated with an existing wireless LAN infrastructure.

SECURITY PROGRAMS

VeriSign's Security Programs can help an organization develop, improve, or communicate security and privacy strategy. VeriSign's team of Certified Information System Security Professionals (CISSPs) augments a client's internal security and privacy staff with on-demand subject matter experts to help align security and organizational strategies with their organization's policies, architectures and technologies. The VeriSign Security Programs includes:

- Policy and Standards Review and Development
- Program Review and Development
- Training and Awareness
- Interim CISO and CPO
- Incident Response and CERT



Policy and Standards Review and Development

VeriSign's Policy and Standards Review and Development evaluates the effectiveness of an organization's existing security policies and standards by comparing them against:

- Business requirements
- Current security practices
- Industry standards of good practice

Based on VeriSign's findings, the company works with its clients to improve their organization's security policies and standards to meet industry requirements and fulfill business objectives.

Program Review and Development

Security programs are composed of business and technology initiatives, as well as market, regulatory and risk forces. The dynamic nature of these programs means that organizations need an effective strategic planning process. VeriSign's Program Review and Development provides expert security and business guidance to help organization's reduce the total cost of security and privacy programs. The service includes:

- Development of practical responses to security and privacy challenges
- Prioritization of near- and long-term security strategies and objectives
- Effective communication of strategic decisions by creating or modifying organizational policies

The result of this service is a well-functioning security and privacy management program across an organization or business unit.

Training and Awareness

Studies show that regular training and awareness building are essential elements to an effective security and privacy program. Employees must understand each program's requirements and how they are expected to comply. Similarly, employees that are unaware of the risks associated with their actions may not fully understand the need for compliance with the policies designed to reduce organizational risk. VeriSign's security and privacy Training and Awareness service addresses organizational "soft" spots by targeting all stakeholders, from security/privacy experts to management and employees.

VeriSign employs a "train the trainer" strategy and develops custom Training and Awareness workshops. Training for the broader user population covers topics such as passwords, acceptable Internet use and other matters of importance to your organization. VeriSign also provides specialized training on regulatory compliance issues (HIPAA, GLBA, EU Safe Harbor, etc.) and technical areas, such as VPN, Intrusion Detection Systems (IDS), and Incident Management and Forensics.

Interim CISO and CPO

With security and privacy functions gaining increased visibility coupled with a shortage of qualified candidates, it can be difficult to find senior security and privacy personnel such as chief information security officers and chief privacy officers. VeriSign's Interim CISO and CPO program provides organizations with security and privacy experts who become part of the client's organization to help them address long-term needs. By providing senior security and privacy staff, VeriSign we can help:

- Define the CISO or CPO functions
- Jump-start stalled security or privacy efforts
- Maintain momentum in existing programs during your permanent CISO or CPO search

Incident Response and CERT

As organizations rely more heavily on their digital assets, threats to those assets are on the rise, making it more important than ever to prepare for information security incidents before they occur. VeriSign's Incident Response and CERT service assists in the creation, implementation and rollout of IR and CERT programs. VeriSign helps its clients create policies and processes to ensure that security incidents are dealt with quickly and effectively. VeriSign creates methodologies to evaluate, mitigate, escalate and contain incidents in a systematic manner. The company also trains its client's staff to ensure their preparedness for potential incidents.

SECURITY TECHNOLOGY

VeriSign's Security Technology services provide "hands-on" assistance for the more challenging areas in information security. Customized to each client's unique requirements, VeriSign spans the range from cyber forensics support to evaluation of emerging technology, including:

- Security Technology Analysis and Integration
- Cyber Forensics Support
- Secure Application Engineering Support
- IDS Engineering and Support

Security Technology Analysis and Integration

With accelerated technological change and shortened application development cycles, security and privacy staff is faced with the challenge of understanding and evaluating an expanding array of new and updated applications, services, and technologies.

VeriSign's Security Technology Analysis and Integration helps organizations assess the critical IT infrastructure elements and then determine the proper installation, configuration and "security-hardening" procedures for each system. VeriSign also provides an unbiased security perspective when evaluating or deploying new technologies such as wireless infrastructures, directory services, e-commerce applications and other leading technology.

Through industry affiliations, VeriSign's consultants have early access to information and training in new technologies and are updated (in real time) on the latest vulnerabilities. This information helps shorten the deployment cycle of new technology into client organizations.

Cyber Forensics Support

VeriSign's Cyber Forensics Support uses the combined skills of the company's forensic specialists, security architects, research and development team and 24x7 Managed Security Services (MSS) operations to handle the needs of any information security investigation. VeriSign's Cyber Forensics Support includes:

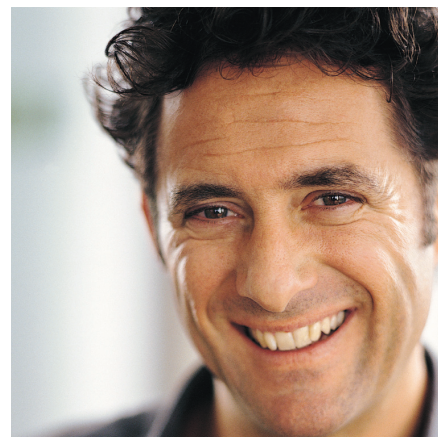
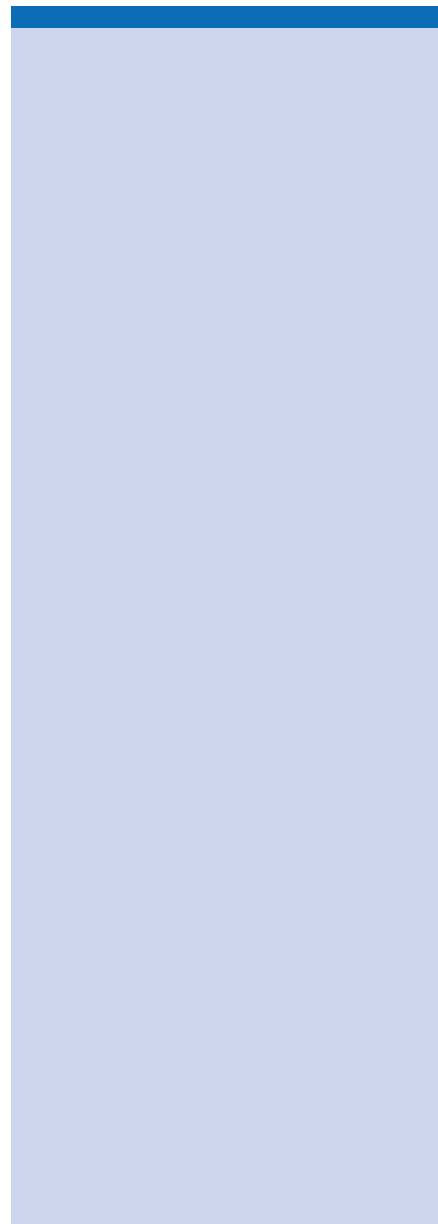
- Investigative Services – Typically required after a hacking episode, the theft of intellectual property, fraud, employee harassment or inappropriate use of network resources. VeriSign identifies, gathers and preserves the electronic evidence needed to take appropriate internal or legal action.
- Legal and Electronic Discovery Services – VeriSign provides expert witness consulting services for companies involved in all types of legal and adversarial proceedings, including assistance with identifying and locating digital evidence relevant to an investigation. More technical services include forensic media analysis, data mining, network monitoring, and digital intelligence services.
- Policy and Program Management – VeriSign will help an organization build an internal forensic capability, establish policies, and provide training.

Secure Application Engineering Support

The Secure Application Engineering Support allows VeriSign to assist a client's internal team throughout the entire application development lifecycle. VeriSign works in all phases of high-level and technical design, product/technology selection, implementation and testing, deployment and performance tuning. This comprehensive engineering support ensures that the correct security controls are adequately addressed in the application design and development process, rather than being retrofitted at a later time resulting in much higher budget and resource costs.

IDS Engineering and Support

The IDS Engineering and Support draws on VeriSign's 24x7 managed IDS security expertise to help organizations design, deploy and tune IDS implementations. VeriSign educates its clients on the proper review process for alerts and assists with IDS training and response planning. On an as-needed basis, VeriSign reviews reports with clients and supplies organizations with a list of high, medium and low threats as they arise. VeriSign can also simulate attacks to test and validate a client's IDS technology and response capability.



About VeriSign

VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence.