

INFORMATION SECURITY CONSULTING SERVICES

Bullzi Security's Information Security Consulting Group is a leader in providing turnkey information security solutions. Through its consulting services and integrated delivery systems, Bullzi Security helps to minimize the threats to its clients' information systems and communication networks. Bullzi Security has developed its own proprietary Information Security Lifecycle methodology in support of its Professional Security Services. Bullzi Security brings a unique set of skills and experience to ensure that its clients receive the most comprehensive, cost-effective information security services available. As an end-to-end information security solutions provider, Bullzi Security offers its clients the full breadth of products and services including:

- Information Security Consulting and Technology Planning
- Information Security Assessments and Audits
- Information Security Policy Review and Development
- Information Security Training and Awareness Programs
- Secure Architecture Design
- Security Products Implementation and Integration
- Computer Incident Response Team (CIRT) w/24 Hour Rapid Response Capabilities
- Investigative and Forensic Services

THE STATE OF (IN)SECURITY

Did you Know? *

That cyber incidents are increasing in number, sophistication, severity, and cost.

Did you Know? *

That the nation's economy is increasingly dependant on cyberspace; this has introduced unknown interdependencies and single points of failure.

Did you Know? *

That a digital disaster strikes some enterprise every single day.

Did you Know? *

That fixing vulnerabilities before threats emerge will reduce risk.

Did you Know? *

That it is a mistake to think that past levels of cyber damage are accurate indicators of the future.

Did you Know? *

That everyone must act to secure their parts of cyberspace.

The threat of a cyber incident is greater than ever before. The threat may be internal; it may come from hackers or crackers, organized crime, or terrorists. Is your organization prepared to respond to this new threat?

** These statements were taken from The National Strategy to Secure Cyberspace, a document released September 2002 by the President's Critical Infrastructure Protection Board.*



INFORMATION IS POWER – PROTECT IT

Information is POWER and only you can protect it. In today's economy, information is your organization's greatest asset. It must be protected from unauthorized access, denial of service, breach of confidentiality, loss of data integrity, etc. Your organization must be prepared to protect, detect and respond to today's cyber attacks. So where should you begin?

Most Bullzi Security engagements start with a security risk assessment or vulnerability testing. The more comprehensive risk assessment takes a snapshot of your organization's vulnerabilities from a physical security, IT security, document security and personnel security perspective. Bullzi Security uses proprietary techniques, based on industry standards (ISO-17799), as well as the most reliable, up-to-date automated security assessment tools, to generate security profiles of essential information systems. The vulnerability testing service focuses on your company's IT exposures. The following sections describe Bullzi Security's professional security services.

VULNERABILITY TESTING

Bullzi Security's Vulnerability Testing service starts with an in-depth technical review of your most critical and sensitive information systems. This service has been designed to help identify network perimeter vulnerabilities that may be used to gain access to networks and systems that process, store, or transmit information. This service includes planning, testing, and analysis centered around transport, protocol, application, and remote access areas. The Vulnerability Testing Service is a precursor to a Penetration Test, which measures a company's real-world vulnerabilities and responsiveness to security attacks. Penetration testing uses the information gathered during the vulnerability scan to attempt to exploit subsets of the vulnerabilities found and to demonstrate how unauthorized access could be achieved

After analyzing the vulnerability and penetration test results, Bullzi Security recommends prioritized, cost-effective corrective measures and security safeguards. This recommendation report serves as the blueprint to help prioritize budget, resources, product selection, and implementation plans. The analysis also establishes a baseline against which security solutions are measured. This baseline enables organizations to track and easily demonstrate security progress to corporate management, investors, and other key stakeholders.

There are a number of technical assessments that can be provided. Some of these are:

- | | |
|---|---|
| <ul style="list-style-type: none">▪ Network (LAN) Assessments▪ Host / Operating System Assessments▪ External Penetration Analysis▪ Firewall and Router Assessments▪ SAS 70 – Type 1 and Type 2 Audits | <ul style="list-style-type: none">▪ Wireless LAN (802.11/WiFi) Assessments▪ Workstation Assessments▪ War Dialing – Modem Assessments▪ Application Assessments▪ Compliance Assessments |
|---|---|



ISO-BASED SECURITY RISK ASSESSMENT

The ISO-based Security Assessment provides a more comprehensive view of the customer's overall security. This evaluation covers all aspects of security using questionnaires, interviews, physical security walk-thru, documentation review, network architecture topology reviews, external port scans, vulnerability scans and penetration testing. After Bullzi Security experts carefully analyze this information, a written report is created, and a second meeting is held to discuss the report, any customer security concerns, and to finalize the comprehensive security plan.

RISK ASSESSMENT AND COMPLIANCE AUDITS

Once a full risk assessment has been completed, a baseline has been established, and its findings implemented, the customer should consider semi-annual or annual audits to ensure compliance with an organization's published information security policies and procedures. Networks are dynamic, and changes take place almost daily. Security audits are as necessary to an organization's well being as its annual financial audits. This external audit will help to make certain that the systems and network remain secure in light of the system and architectural changes. Bullzi Security offers Basic and Advanced security audits.

INFORMATION SECURITY POLICY – PLANNING AND DEVELOPMENT

The Security Policy Planning & Development service provides businesses with a standard "Best Practices" Security Policy template. The service identifies, recommends, and implements appropriate security policy and policy-specified safeguards to help protect your customer's information assets. Additionally, a security professional will tailor a "standard security policy" to meet specific business needs. If the organization currently has an information security policy, this service will include a review of the existing policy and will make recommendations to bring the current policy up to a "Best Practices" level.

The process begins with an interview between the security consultant and the customer. Following the interview, the customer will be provided with a draft written policy. This policy covers three major areas:

- **Logical security.** Includes system access control (i.e. log-in); password policy; software configuration and change control. It also includes use of anti-virus protection; acceptable use; data security and privacy; Internet access; e-mail usage; data availability; and data integrity.
- **Managerial security.** Includes security awareness training; personnel security; organizational structure (division of responsibility); policy enforcement; incident handling procedures; and separation of duties.
- **Physical security.** Includes building access control; restricted access to computer facilities (e.g. server rooms); and computer location. Depending on the desired scope, it may also cover such things as fire suppression systems, facility construction, or air-conditioning.



TECHNOLOGY PLANNING

The Technology Planning Services assist customers in selecting the proper security solution from a broad range of product offerings. Bullzi Security consultants provide on-site consulting services to help a customer select and design a robust security solution. Bullzi Security offers technology planning services for the following security safeguards:

<ul style="list-style-type: none">▪ Firewall Design▪ Intrusion Detection & Prevention Systems▪ Virus and Malware Protection▪ Content / URL/SPAM Filtering▪ Encryption	<ul style="list-style-type: none">▪ Two-Factor Authentication▪ PKI / LDAP / X.509▪ Physical Security▪ Biometrics▪ RADIUS / TACACS Servers
---	---

INFORMATION SECURITY TRAINING PROGRAMS

Bullzi Security offers security training for every audience, from your front-line employees to the IT department and upper management. Our security training services focus on the following areas:

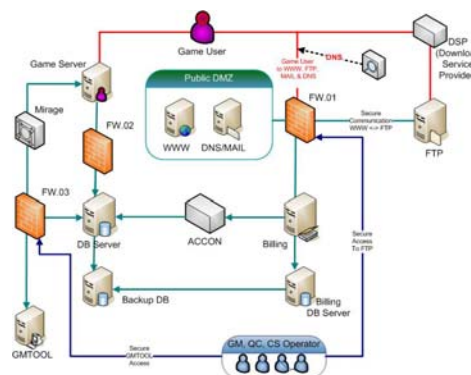
- **Awareness Training** – The Information security policy is the cornerstone of any enterprise security solution, but if end users don't know about the policy, or aren't up to speed on its components, then the policy serves no purpose. Your information security policy is the blueprint for acceptable system use and your people need awareness training to understand this and their role in your security policy. This training program focuses on:
 - Comprehensive explanations of system use
 - The reasons why you must protect your information assets
 - The types of threats, including social engineering
 - The penalties for non-compliance
- **IT Security Training** – As you know, your IT staff are the linchpin for ensuring that your network runs smoothly, and now more than ever, your IT people need a thorough understanding of how IT security works. That's why Bullzi Security's IT Security Training service offers a variety of Information Technology-oriented training options. Bullzi Security educates, informs, and guides your IT personnel in planning, designing, and implementing best security practices. Our approach to training includes real-world instructions and tools to help prevent the misuse of hardware, software, and processes that could result in compromised security.

All courses come complete with experienced subject matter expert instructors and presentation media and materials designed to minimize production down-time during training. We offer tailored instruction that suits your IT staff needs and levels of expertise, as well as one-on-one training, or group training. Training can be provided through the traditional classroom environment, or via a web-based, self-paced program.



SECURE ARCHITECTURE DESIGN

The Bullzi Security design team can help your organization design a secure network infrastructure. Through the use of firewalls, intrusion detection systems, strong authentication mechanisms, VPNs, etc., your organization can achieve a higher level of security, but the proper placement, configuration and interoperability of the various devices and appliances is essential. Other key areas to consider are content/URL filtering, high-availability or redundant solutions, VLANs, centralized logging servers, secure subnet segmentation, router controls, dial-up access, etc. Bullzi Security has a team of professionals that have the expertise in each of these areas. They have the credentials and product certifications on each of the technologies that they deploy. In addition to design, configuration and implementation, our security professionals can train your staff in all areas of secure architecture design.



COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The Bullzi Security Computer Incident Response Team (CIRT) has the experience and knowledge to respond to today's network intrusions and adverse computer events. Bullzi Security provides expert guidance in the area of detection, containment, internal reporting, external disclosure, and investigation. Computer crime investigation and computer forensics are esoteric fields, and few individuals or corporations have the depth of experience as Bullzi Security's CIRT and Cyber Crimes Unit.

Even in the most secure computer environment, adverse events do happen. Computer security incidents are occurring at an ever-increasing rate, and the ability to respond to and investigate computer security incidents is essential. Unfortunately, even with all of the proper training, you may have difficulty effecting a successful response due to the lack of experience. The CIRT brings that experience! The CIRT is placed on retainer prior to a security breach. Should an adverse event occur, the CIRT is prepared to be on site within 24 hours of notification. Once our team responds on site, they evaluate the situation and assign an incident classification and severity level to the incident. This helps the team to gather the necessary resources and to advise the customer of the overall impact to their business. The CIRT members can also provide liaison support for the law enforcement and media relations.

During an investigation, critical evidence needs to be obtained and analyzed. This is the basis of computer forensics. A forensic examination encompasses the analysis of computer-related evidence after the fact, or if possible, in real-time during an intrusion. Because of the substantial amount of litigation that involves technology, the need for qualified computer forensics is on the rise. The Cyber Crimes Unit is comprised of recognized experts in computer crime investigations and the computer forensics industry. Bullzi Security has a state-of-the-art forensic lab in its New Jersey office.



INDUSTRY-SPECIFIC SOLUTIONS

The Bullzi Security Consulting team has been in the business of helping organizations protect their valuable information assets in all industries for many years. Supporting our clients' efforts to achieve HIPAA, SOX, GLBA, NERC or GISRA Compliance, is a natural extension of our services.

Healthcare Insurance Portability and Accountability Act (HIPAA)

Bullzi Security's HIPAA Security & Privacy team is comprised of professionals who possess advanced certifications and relevant experience in Healthcare Administration, Privacy Administration, Security Solutions, Training/Education, Program Management, and the development of secure, end-to-end electronic commerce solutions (EDI). Bullzi Security offers security services tailored for this particular industry, including HIPAA Assessment services.

A HIPAA Assessment enables healthcare organizations to get a fast, accurate, and in-depth overview of their HIPAA readiness from a security, privacy, and EDI standpoint. Conclusions and findings are provided in a cost-effective security report ("gap analysis") tailored to their unique environment. The following HIPAA Assessments are available:

- Healthcare Practice Assessment—Designed for a single-location hospital.
- Healthcare Enterprise Assessment—Designed for organizations with a primary hospital site, which houses main operations and IT network infrastructure, and has multiple smaller sites.
- Healthcare Integrated Delivery System Assessment—Designed for a large multi-location hospital or integrated healthcare network that has more than one primary site, such as affiliated hospitals, as well as several smaller sites such as doctor's offices, clinics, or nursing homes. Each primary site has its own comprehensive operational and IT network infrastructure.

HIPAA University, a subsidiary of Bullzi Security, developed the first HIPAA Compliance Program in the industry (in late 2000), and is now shipping version 6, which makes our HIPAA Compliance Program (effectively a Program Management Methodology) the most thorough and easy to use solution in the industry.

Our current suite of products and services include:

- Comprehensive HIPAA Compliance Program (Hospitals, Clearinghouses, and Health plans)
- HIPAA Compliance Program for Medical Practices
- HIPAA Training Courses (over 50 titles to choose from)
- HIPAA-U.com (our virtual community for customers to collaborate regarding HIPAA efforts)





Gramm-Leech-Bliley (GLBA)

The Gramm-Leech-Bliley Act (GLBA) was drafted in 1999 to provide strict regulation related to the privacy of financial data. Under the act, financial institutions, insurance companies, credit card companies, etc. are required to safeguard personally identifiable financial information and reveal their privacy policies to new customers, regardless of whether the financial institutions will share the information. Major steps to ensuring compliance include ensuring security and confidentiality of customer information and the protection against unauthorized access to or use of such information.

Bullzi Security is well positioned to help our financial clients achieve compliance with this act. We can help our clients assess their current security exposure as well as design and implement security policies, processes, procedures and countermeasures, to mitigate the looming threat.

Sarbanes-Oxley Act (SOX)

Just as with HIPAA and GLBA, Bullzi Security has a team of security professionals who understand the requirements established by the Sarbanes-Oxley Act (SOX). Section 404 of SOX requires public companies to ensure the accuracy and reliability of their financial reporting systems. Since, in most cases, these financial reporting systems are accessible from the internal LAN, a number of security controls needs to be implemented and maintained. SOX compliance starts with an assessment that evaluates the current controls. Bullzi Security uses the Cobit Control Objectives to help our clients achieve SOX compliance. The sanctions for non-compliance can be financial penalties or criminal charges.

North American Electric Reliability Council (NERC) Standards

The North American Electric Reliability Council (NERC) was formed by the electric utility industry in 1968 to promote the reliability of their generation and transmission systems. In 2002, NERC added the Standard 1300 – Cyber Security to its charter of ensuring that bulk electric systems in North America are reliable, adequate and secure. Standard 1300 has been enhanced and is now known as Standard CIP-002 through 009. Bullzi Security understands this new regulation and can assist its electric utility clients with overall compliance.

Government Information Security Reform Act (GISRA)

In 2000, the government enacted new legislation, the Government Information Security Reform Act (GISRA), which requires Federal agencies to assess and report on the security needs of their systems and networks as part of their budget requests to the Office of Management and Budget (OMB). Until the release of the National Strategy to Secure CyberSpace, GISRA had no teeth, but now the strategy recommends that OMB reject agency budgets that do not include plans to boost protection and address security shortfalls. Federal agencies must take decisive action when it comes to their information infrastructure. As stated in the National Strategy for Homeland Security, “Unless we act to prevent it, a new wave of terrorism, potentially involving the world’s most destructive weapons, looms in America’s future. It is a challenge as formidable as ever faced by our Nation.” We need to be prepared! We need to protect our systems and networks. We must be ready to prevent, detect and respond to today’s new cyber threat.



WHO IS BULLZI SECURITY?

Bullzi Security is an organization built on strong values, extensive experience, agility, and a team-oriented approach to meeting client needs. Bullzi Security is a publicly held Nevada corporation with operational locations in New Jersey, New York, Florida and Toronto. Bullzi Security consultants hold the following industry certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified Protection Professional (CPP)
- Certified Fraud Investigator (CFI)
- Certified In Homeland Security (CHS-III)

In addition to industry certification, Bullzi Security consultants are certified in following products:

- Certified Checkpoint Security Administrator/Engineer (CCSA/CCSE)
- Certified Rainwall Engineer
- Certified Nokia Security Administration (IPSO and VRRP)
- Cisco Certified Network Associate (CCNA)
- Certified ISS Database, Internet Scanner and Real Secure IDS Engineer (ICE)
- Certified Entrust PKI Administrator & Engineer
- Certified EnCase
- Tripwire Certified
- Network Flight Recorder Certified
- ELRON Internet Manager Certified
- Certified Ademco (Security System) Installer
- Certified Northern Computer Card Access System Installer

It is our goal to become further respected by our clients, trading partners, and peers as the security consulting firm that is most knowledgeable, professional, and cost-conscious as we tailor security solutions to meet individual client requirements. No one takes more job ownership in achieving these goals than our professionals.



For more information about Bullzi Security, Inc., please contact our Florida corporate headquarters at (407)562-1864 or (888) 763-2279 or via website: <http://www.BullziSecurity.com>.