TruSec Consulting

Information Security
Risk Management
Compliance Assurance

Information Security Assessment Services

INFORMATION SECURITY ASSESSMENTS

A WEAK, UNSAFE TECHNOLOGY INFRASTRUCTURE WON'T SUPPORT YOUR LONG-TERM BUSINESS GOALS

BACKGROUND

The success of your business depends heavily on your Information Security and Risk Management road map. Hence, you must assess your road map to validate its strength and ensure it supports the business strategic initiatives. Information Security Assessments help management create appropriate strategies and controls for stewardship of information assets. Periodic assessments are a requirement of many compliance initiatives to verify that new system implementations, or changes to existing systems, have not introduced new, unmitigated vulnerabilities to the organization. TruSec can assess the overall security of your organization and provide a valuable baseline for determining appropriat e safeguards. TruSec uses globally recognized standards and frameworks to understand and document yourexposure to threats that may cause loss of information confidentiality, integrity, availability, accountability and assurance.

WHY TRUSEC

When you engage with TruSec for your information security assessments, you gain access to a team of experts with many years of professional experience in the design, implementation, support and auditing of enterprise-class IT systems and their associated security, privacy and compliance initiatives. Because of our unmatched skills and expertise, we are able to dig in deeper where others only scratch the surface. Client deliverables are also submitted to internal peer review to ensure the governance, risk and compliance goals of your organization are taken into account, so that every recommendation we make is not only comprehensive but also relevant to your environment. Only TruSec can provide the right combination of skills, experience and methodology that provide the best value proposition to our clients. Let the TruSec team build and maintain a sustainable Information Security and Risk Management road map that supports your business strategic initiatives.

VULNERABILITY ASSESSMENTS

Our team will help your organization understand the security and risk posture of its information systems by inventorying, quantifying and prioritizing the vulnerabilities of your information systems and determining is these can be exploited by an attacker to compromise targeted systems or used to gain access to sensitive information.

info@truseccconsulting.com | www.truseccconsulting.com | 855 TRUSEC 1

PENETRATION TESTING

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

WEB AND MOBILE APPLICATION VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Web and Mobile application security reviews are composed of both comprehensive automated analysis and targeted manual testing techniques. Our testing methodology ensures the uniform detection of common vulnerabilities such as input injection, improper session management, information disclosure and other categories mentioned within the current OWASP Top Ten vulnerability rankings and beyond. All of our deliverables include detailed descriptions, proof-of-concept demonstrations and a remediation roadmap to successfully address discovered vulnerabilities.

SOCIAL ENGINEERING / SECURITY AWARENESS ASSESSMENT

TruSec's consultants can help assess the effectiveness of your security awareness training program by attempting to gain access to an organization's systems through non-technical means. Social engineering is a critical component of an information security assessment as it helps to identify areas of weakness in an organization that cannot be addressed through technical solutions such as firewalls and intrusion prevention systems.

PHYSICAL SECURITY REVIEW

The integration of physical security and information security can no longer be overlooked. Not only is physical security a requirement of most compliance initiatives, it is a requirement of a truly complete information security protection plan. TruSec's physical security assessment provides this integration by validating existing physical security access controls, providing recommendations for methods to improve integration between physical and information security, and implementing the recommendations.

WIRELESS SECURITY REVIEW

An analysis of an organization's overall wireless security posture along with benchmarking information of the configuration of the WLAN networks against industry best practices. TruSec will attempt to identify authorized and unauthorized wireless networks, conduct a review of your organizations approved wireless infrastructure and test for vulnerabilities associated with its implementation.

SENSITIVE DATA DISCOVERY

The first and most important step to reducing information risk is to identify where your data resides so that appropriate measures are taken to protect it. Our assessors can discover unprotected NPI and PHI across the enterprise including networked and local drives as well as databases. The information is classified based on content and provided in a concise report that can help you plan for mitigation strategies to protect the discovered sensitive data.