whitleypenn

Cyber Defense Initiative

Cyber Defense Initiative

Security threats, vulnerabilities, and data breaches have become a top priority for boards and senior executives around the world. The sophistication of attackers and complexity of the threats require organizations to not only implement sound security technologies, but also have robust controls and processes around information security. As a part of its Cyber Defense Initiative, Whitley Penn is committed to helping clients evaluate the adequacy of the technology, controls, and processes implemented to secure your information assets and provide valuable recommendations for improving your organization's security posture. Our accomplished information security professionals have experience advising clients in a variety of information security and privacy areas, including:

Vulnerability Assessment

A vulnerability assessment is the process of discovering, documenting, and quantifying security vulnerabilities found within your environment. A vulnerability assessment is intended to be a comprehensive evaluation of the security of your vital infrastructure, endpoints, and IT assets. It gives insight into system weaknesses and recommends the appropriate remediation procedures to either eliminate the issue or reduce the weakness to an acceptable level of risk.

Vulnerability assessments typically follow a structured methodology, which should include the:

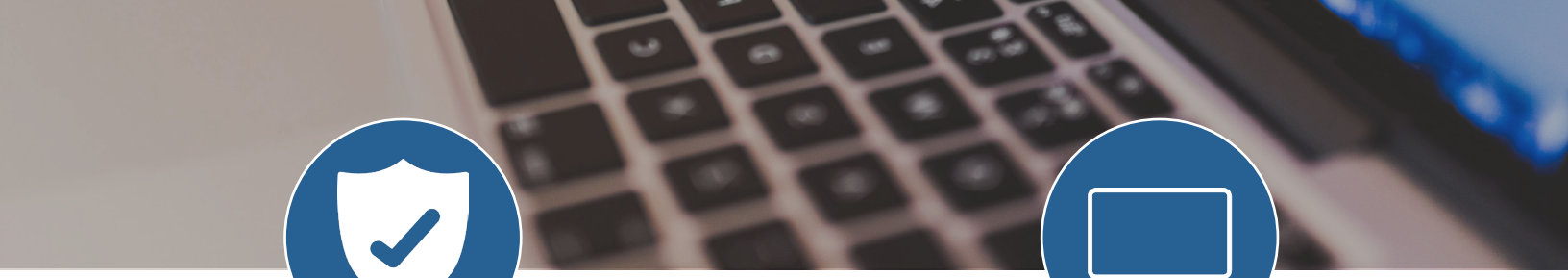
- Identification and cataloging of assets (systems, infrastructure, resources, etc.);
- Discovery and prioritization of the security vulnerabilities or potential threats to each asset; and
- Reporting on the recommended remediation or mitigation of vulnerabilities to reach an acceptable risk level.

Penetration Testing

A penetration test attempts to simulate the actions of an external or internal attacker who is trying to exploit the vulnerabilities present within your organization. A qualified pen tester uses a combination of tools and techniques to bypass the existing security controls of the target organization. The goal is to gain access to sensitive systems and information.

The methodology followed by our pen testers is inherently less structured to allow for rapid adjustment during testing. However, most of our methodology typically follows these key steps:

- Determination of the scope and testing objectives;
- Targeted information gathering and reconnaissance;
- Identification and exploitation of weakness to gain and escalate access;
- Demonstrate completion of the testing objective; and
- Clean up and reporting.



Phishing Campaign

Mature information security technology and controls are only as good as the people that are responsible for them. A recent study found that over 90% of data breaches were the result of a combination of phishing attacks and social engineering. To evaluate the effectiveness of your security awareness program, a phishing campaign can help you know where you stand.

Phishing campaigns test your employees' propensity to click on email phishing lures with an effort of obtain system credentials utilizing open source technologies and false emails accounts with an endeavor of representing a reputable source. Obtained credentials will be reported for determining the effectiveness of users' awareness of phishing email avoidance.

Cyber Security Risk Assessment

For most businesses, compliance with IT requirements from regulations, standards, and contractual obligations is unavoidable. Using our understanding of a broad range of information security regulations, risks, and best practices, we can perform a cyber security risk assessment and make recommendations to help you improve your security posture and compliance efforts. We are prepared to assist you in your efforts to comply with a broad range of requirements, including:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA) /Health Information Technology for Economic and Clinical Health Act (HITECH)
- International Organization for Standardization (ISO) 27001
- National Institute of Standards and Technology (NIST) Special Publication 800-53/800-171
- SOC 2 Trust Services Criteria
- General Data Protection Regulation (GDPR)
- Federal Financial Institutions Examination Council (FFIEC)

Whitley Penn is committed to working with our clients to assess their current controls, develop solutions that achieve compliance, protect your data, and manage ongoing threats. As a result of our Cyber Defense Initiative, we will help you improve your security architecture; strategy; governance, risk, and compliance; threat intelligence and vulnerability management; information protection and privacy; and cybersecurity training and end-user testing.

Whitley Penn continues to be one of the region's most distinguished public accounting firms. With a strong base in Texas and a worldwide network affiliation via Nexia International, the firm is strategically positioned for continued growth both locally and internationally. Whitley Penn has been consistently recognized as "One of the Top 100 Firms in the U.S." and "Best of the Best" by *INSIDE Public Accounting*.

For more information on Whitley Penn, please visit whitleypenn.com.