CYBER SECURITY SOLUTIONS

Continuous Protection for the Enterprise

Today's rapid changes of technology, cyber threats, numerous breaches and theft of personal information has brought about an increased need for legislation for the protection of data and it is now paramount for any organization to implement a comprehensive cyber security plan -- no matter how small or large.

Overview

The implementation of cyber security policies requires in depth analysis of threats from inside and outside the organization by detail assessment of points of egress and ingress in any organization's network and the handling of security and data at those points. Insider threats can come from employee negligence, lack of knowledge or by malicious or politically motivated employees. Outside threats can come from hackers, malware, phishing attempts, thieves and/or competing vendors.

No matter where the threat comes from, the cost of a breach could be considerable and sometimes unquantifiable when you consider loss of customer trust, loss of trade secrets, confidential Human resource information that most likely will result in loss of future revenue to any organization. The cost to organizations such as Law Firms, Health organizations, banks and financial institutions who are in the "trust business" can be in the many millions of dollars, loss of clients and reputation and can result in civil litigation and additional compliance requirements. As one example, Law Firms that fail to safeguard client or customer data face legal liability for negligence, breach of fiduciary duty and breach of contract.

So how does an organization protect itself from these various cyber threats?

What we do?

We can help. Trident, Inc. , has been providing comprehensive IT services to small and large commercial and government organizations since 1983. Using the latest Cyber technologies tools and practices, Trident delivers to its clients, the latest, most innovative methodologies to systematically analyze and review your environment and come up with real world implementable solutions and policies to minimize

Trident, Inc
1220 North Fillmore St. Suite 400 Arlington, VA 22201
Tel: 571.482.7131 | **info@trident.net** | **www.trident.net**

Contact Us for a free consultation session for all your specific cyber security needs.

info@trident.net

or

Call us at 571-482-7131

cyber breaches and data theft.

The Trident Cyber Methodology (TCM) consists of three distinct levels of analysis to yield a comprehensive examination of a client's environment. The first phase of the engagement is the Enterprise Security Audit (ESA) which is an audit of IT operations from a security perspective and is based on Center for Internet Security Critical Security Controls (https://www.cisecurity.org/controls/). Once our ESA is completed, a plan is developed to address/ remediate the findings from the ESA and re-enforce your network. We then discuss how best to proceed with the appropriate Penetration Tests from external and internal actors or other tests as needed for Phase two of the engagement. The number of devices and the number of access points to the network determines the complexity and extensiveness of these tests.

The third and last Phase of the engagement includes detail analysis and verification of policies and procedures that must be implemented to prevent future attacks and threats. This phase includes checking and investigation of employee computer usage and training on cyber security practices to prevent threats such as phishing, viruses and ransomware which can cause substantial damage and loss to any organization's systems and data. Additional tests and training can be designed and implemented on a per client basis.

CYBER SECURITY PLANS

Enterprise Security Audit Documentation Review--Remote	√	√	√
Internal Vulnerability Assessment	√	√	√
External Penetration Test (Black Box)	√	√	√
ESA Retest	√	√	√
Blackbox Retest	√	√	√
Compliance Remediation Support	√	√	√
Social Engineering - Remote		√	√
Wireless Penetration Test -- On Site		√	√
Expanded Compliance Remediation Support		√	√
ESA On Site Operational Review			√
Second Internal Vulnerability Scan			√
Social Engineering -- On Site			√
Additional Penetration Test			√
Web Application Penetration Test			√
Web Application Penetration Retest			√
Expanded Compliance Remediation Support			