Problem Case Study || Government

Cybersecurity holes expose government institutions and critical infrastructure. Regulatory mandates such as FISMA, HIPAA and SOX as well as Duty of Care require agencies to implement extensive information security programs while protecting the privacy of US citizens.

The US Navy and US State Department require workforce performance improvements and internal security threat mitigation. The misuse and abuse of network resources by human capital is a significant source of risk and productivity loss within these entities. Careless or negligent conduct by employees and contractors reduces resource availability and can compromises security policies.

The Solution

Both entities turned to Pearl Echo.Suite for its ability to manage the increasing risk posed by government employees and contractor conduct. Pearl Echo protects data-in-motion through settings defined to govern the Internet access permissions of users. Specific cybersecurity privileges can be applied to individual users, groups of users or computers. Pearl Echo will identify when specific content is transmitted in various segments of the Internet and will highlight or block transactions containing patterns defined for the user. Pearl Echo will examine attachments in real-time and provide full analysis of clear and encrypted data prior to it becoming data-in-motion.

Pearl Software provides Government Agencies with a NIST Guide to fully support their efforts in documenting cyber security policy. The NIST Framework helps agencies align their cybersecurity activities with their agency requirements, risk tolerances and resources. The Pearl Software NIST Guide provides a tool to match Pearl Software's cybersecurity product capabilities to NIST Framework categories.

Success in the Field

Navy and State have been using Pearl Echo.Suite since 2005 and 2003, respectively. Both have successfully mitigated risk by stemming inappropriate and illegal use of the Internet within their respective entities. The agencies use Pearl Echo to help satisfy portions of the Protect, Detect and Respond functions of the NIST Framework. Specifically, Pearl Echo is applied to the PR.AT-1, PR.DS-2, PR.DS-5, PR.DS-6, PR.PT-1, PR.PT-4, DE.AE-1, DE.AE-2, DE.CM-1, DE.CM-3, DE.CM-8, DE.DP-4 RS.AN-3 Framework categories.