

A Case Study: How HTSI's Cyber Security Vulnerability Assessment Helped a Communications Network Company to Identify, Mitigate and Manage Risks to Its Critical Infrastructures

It's all about managing risk:

"Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, must be performed with a frequency depending on risk, but no less than annually."

– Federal Information Security Management Act - 2002

The Client: A Communications Network Company

The client, a communications network, manages communications between various enterprise networks and manages data processing and dissemination for end users.

Scope

Faced with the emergence of new security recommendations and regulatory compliance requirements for the communications industry, and emerging cyber threats to its enterprise infrastructure, the company needed to determine the vulnerability of its infrastructure, what remediation efforts were required to bring it into compliance and how to focus remediation efforts based on available resources.

The company contracted with HTSI to provide a **Cyber Security Vulnerability Assessment**

of its enterprise systems. HTSI used its proven assessment methodology to collect security-related information across many distinct security domains and to report on the overall compliance level of the company's cyber security program.

HTSI utilized automated tools, coupled non-technical assessment methodologies (inspections, document reviews and observations), to audit current technologies, processes and personnel to determine the depth of its defense strategy, and whether each meets regulatory compliance and best practice standards.

Additionally, HTSI reviewed the the company's enterprise boundary protections, network and infrastructure design and configuration, computing environment, continuity of operations, customer identification and authorization, human resource practices, physical and environmental controls, and vulnerability and incident management.



HTSI's **Cyber Security Vulnerability Assessment** examines the three critical facets of the organization's cyber security program – People, Processes and Technologies.

HTSI Employed a Holistic Audit Approach for Vulnerability Assessments

HTSI's Cyber Security Vulnerability Assessment team examined the three critical facets of the organization's cyber security program – People, Processes and Technologies.

People

- Evaluated whether personnel authorized on the network were properly aligned to their specific roles for both the operational capabilities and the security capabilities.
- Assessed whether the cyber security awareness level within the organization aligned to the security plan.
- Evaluated whether the personnel followed existing security policies and procedures.

Processes

- Observed whether cyber security policies and procedures were documented and in place within the organization.
- Evaluated logs and records to validate that policies and procedures were followed.
- Determined whether physical and environmental controls were adequate, in place, tested and maintained to prevent an incident or to mitigate and reduce damage from an incident.

Technologies

- Imaged systems to ensure system restoration in the event of an incident.
- Gathered logs and security-related data for correlation and analysis.
- Assessed system configurations against best practice technical standards.
- Evaluated vulnerability and patch management status.
- Analyzed server, workstation, router, and switch configurations.

The Assessment and Recommendations Report

HTSI's cyber security experts aggregated the personnel, process, and technology data across the regulatory security domains to produce a detailed report of the compliant and non-compliant security controls. The executive summary provided a high-level report on the current security posture of the company's network and recommended remediation requirements based on identified security deficiencies.

The detailed report provided a system-by-system review of the security posture and identified non-compliant controls that needed to be addressed. Additionally, the report identified deficiencies within the physical location in regards to human resource practices, physical and environmental controls and industry best practices.

Each of the non-compliant controls was evaluated with a risk assessment aligned with NIST 800-39 Risk Management Framework. The risk assessment provided a structure on which to build a roadmap for removing and/or diminishing revealed risk areas through either immediate or future remediation programs.

Immediate and Lasting Benefits

HTSI's **Cyber Security Assessment** provided the customer with detailed information about current compliance gaps associated with the required regulatory standards in an easy-to-interpret document. This document helped the the customer to prioritize its remediation requirements, based on available funding, remediation complexity and business imperatives.

Armed with this knowledge, the company was able to further develop and refine its overall Cyber Security Program, including creating a risk management framework, identifying remediation processes and developing an overall mitigation roadmap. The company was then able to focus its limited resources and time towards higher-risk areas and on quick-fix, low-cost items that satisfied immediate security concerns.

For More Information:

Visit our website www.honeywell.com/HTSI or contact a HTSI account manager to learn more about:

- HTSI's Cyber Security Vulnerability Assessment
- Learn more about HTSI's Critical Infrastructure Protection Program
- Learn how Honeywell Security Solutions can help to manage risk at your site

Aerospace Defense & Space

Honeywell Technology Solutions Inc.

7000 Columbia Gateway Drive

Columbia, MD 21046

Tel: 410-964-7000

www.honeywell.com/HTSI

www.honeywell.com

The Honeywell logo, consisting of the word "Honeywell" in a bold, red, sans-serif font.