Industry Case Study

Healthcare Industry

CYBER SECURITY & RISK MANAGEMENT SOLUTIONS

LYNX TECHNOLOGY PARTNERS

HEALTHCARE SOLUTIONS

Many companies in the healthcare market struggle with compliance projects and finding the time and knowledgeable resources, as-well-as the budget, to adhere to government regulations in a timely manner.

For this particular healthcare organization, finding a company that they could quickly develop a close relationship with as-well-as build trust in performing the necessary tasks within a very rigid timeline became a daunting task.

enter... *Lynx Technology Partners*

Our client, one of the largest, independent healthcare technology companies in the United States, was contracted with a major Center for Medicare and Medicaid Services customer and was required to become FISMA compliant within a year. Not only was this paramount to keeping this customer and the multi-million-dollar contract but with this accreditation, the client would be capable of growing this line of business. This type of accreditation, given where they were in the process, was estimated to take several years. By the time Lynx was on-boarded, we had 9 months to complete our audit.

The accreditation included all aspects of Security Assessment and Authorization (SA&A), Information Assurance (IA), and Information Security (InfoSec) and focused on the configuration and research of the network and generation of over 30 organizational policy and procedure documents. The Lynx Team created the System Security Plan (SSP), Risk Assessment (RA), and Disaster Recovery Plan (DRP) after thoroughly evaluating and guiding the client on Best Business Practices, CMS requirements, Federal Systems Security Management Act (FISMA) and the National Institute of Science and Technology (NIST) regulations.

The Lynx Team dedication and work principles allowed the Information Assurance team to meet the requirements of CMS regulations and complete a two-year project in just nine months. This IA team was also an integral part of implementing all Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGs) and walked the client through the rigorous implementation and documentation of STIG requirements. The Lynx Team successfully submitted the SSP, RA, and DRP to senior management and facilitated an internal and external C&A audit. Lynx also managed all Plan of Action and Milestones (POA&Ms) and Corrective Action Plans (CAPs) for the audit findings.

Results at a Glance

We're here to help.

- Developed over 30 organizational policies and procedures
- Created the System Security Plan (SSP), Risk Assessment (RA), and Disaster Recovery Plan (DRP)
- Helped with the network configuration and DISA STIGs in the environment
- FISMA & NIST compliant environment within 9 months
- Saved a $50 million contract

what we do *differently*

Lynx Technology Partners is the trusted Information Security and Risk Management Advisor that customers in highly regulated industries worldwide depend on to improve security posture, facilitate compliance, reduce risk, and refine operational efficiency.

With world-class skills and knowledge capital built over 30 years, Lynx security experts help customers recognize and control IT-related risks and maintain compliance with major industry and government standards.

why*Lynx?*

Lynx provided a Project Manager (PM), along with a nine-member team to lead the project of obtaining compliance within the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) for a HIGH category system. The Lynx PM provided detailed weekly and monthly status reports to the Executive Team and interfaced regularly with key stakeholders. The team conducted Certification and Accreditation (C&A) compliance testing in accordance with the CMS ARS based on NIST SP 800-53.

Lynx created system documentation including corporate, enterprise, and departmental security policies and procedures. The documentation created was key in developing and writing the System Security Plan (SSP) which included data flow and network diagrams, along with software and hardware lists. Security Technical Implementation Guides (STIGs) and Industry Best Practices were implemented and used to create and document System and Network Baselines. Updated STIGs, Industry Best Practices, patch management, vulnerability scans, and compliance scans were used to maintain the Baselines.

Lynx advised the customer on compliant information security solutions to meet and exceed the CMS, ARS, and NIST requirements. The team provided guidance and assistance for the implementation and monitoring of security tools to include vulnerability and compliance scanning such as Titania Nipper Studio network security software, Tripwire CCM for configuration compliance, Tripwire IP360 vulnerability and risk management solution, and IBM Q-Radar SIEM. Team members assisted in the testing, troubleshooting, and education of several implemented tools. Lynx also provided guidance in the set up and implementation of continuous monitoring for the system.

Formal Information Security and Audit Preparation Training was developed for three separate levels of employees consisting of Management, Technical, and General personnel. This training was delivered over a two-week period to three geographically disbursed locations. Additional informal training was provided to the Management Staff, Compliance Team, and Information System Security Officer (ISSO) on baseline creation and management and the mitigation of issues arising from vulnerability and compliance scans.

IT-Related Regulations

Healthcare organizations are facing an increasingly complicated regulatory environment.

Lynx can help with:

- HIPAA (Health Insurance Portability and Accountability Act)
- HIPAA HCFA Internet Security Policy
- HITECH ACT
- NIST SP 800-66 (Introductory Resource Guide for HIPAA)
- CMS Core Security Requirements (CSR)
- CMS Information Security (IS) Acceptable Risk Safeguards (ARS)
- CMS System Security Plan (SSP) Methodology
- CMS Information Security (IS) Business Risk Assessment (RA)
- CMS Business Partners Systems Security Manual (BPSSM)
- PCI DSS v3.1
- EHNAC
- SOC

in*Conclusion*

Lynx conducted an internal audit and then led the coordination of an independent audit conducted by external auditors. The internal audit consisted of Vulnerability Assessments, external/internal Penetration Testing, Risk Assessments, documentation review, and interviews of system and control owners. After completion of the independent audit, team members assisted in creating, managing, and implementing Corrective Action Plans (CAPs) to mitigate all findings within the required timeframe resulting in a successful compliance audit.

As a result of Lynx efforts, the client achieved FISMA compliance within nine months, creating a brand-new environment with new policies and procedures resulting in client revenue of over $50M a year and the potential for future government contracts. As an extension of client resources, Lynx helped them reach their goal and keep their customer happy and compliant as well as grow the line of business. Lynx's ability to produce quality work within a very aggressive timeline and resulting in FISMA compliance within 9 months was invaluable in the client's eyes.

LYNX TECHNOLOGY PARTNERS

Global Headquarters
244 5th Ave Suite 1220
New York, NY 10001

New York | Pittsburgh | Washington, D.C.

800.314.0455
www.LynxTechnologyPartners.com
InsideSales@LynxTP.com