Case Study: Secure GCCH Enclave Establishment for DoD Contractor

Client Profile

ZYX Corp. is a mid-sized training technology company with approximately 200 employees and annual revenue of $30 million. The company is growing quickly. Facing a growing demand for secure IT infrastructure to meet DoD compliance standards, the company recognized a critical need to enhance its cybersecurity posture. Because of limited IT resources and a tight budget, ZYX Corp. chose to implement an enclave as a cost-effective way of implementing a certifiable solution that did not negatively impact the productivity of those employees who were not involved with DoD contracts and Controlled Unclassified Information (CUI).

Challenges and Pain Points

ZYX Corp. encountered several obstacles in achieving its cybersecurity goals. A lack of dedicated IT security staff and a history of failed enclave implementations hindered their progress. Moreover, increasing pressure from customers to demonstrate 800-171 compliance, coupled with a negative Supplier Performance Risk System (SPRS) score, underscored the urgency of the situation. The company required a partner capable of providing comprehensive support, including technical expertise, project management, and ongoing guidance.

Solution

To address ZYX Corp.'s challenges, our company proposed a tailored solution centered around the Microsoft Azure Government Cloud High (GCCH) environment. Our approach involved architecting a secure enclave comprised of key components:

- **Microsoft Azure GCCH:** Providing a robust, compliant cloud platform.
- **Microsoft Office 365 Government:** Enabling secure collaboration and productivity.
- **Enterprise Mobility + Security (EMS):** Safeguarding mobile devices and applications.
- **AvePoint Backup:** Ensuring data protection and recovery.
- **Virtual Desktop Infrastructure (VDI):** Delivering secure remote access.
- **Microsoft Purview:** Providing comprehensive information protection and governance.

- **Custom-Developed CONOPs:** Outlining operational procedures for the enclave.

Our team collaborated closely with ZYX Corp.'s small IT staff to implement and configure these components, creating a secure environment for handling CUI. To minimize disruption, the initial enclave focused on a subset of employees with critical CUI access.

Implementation and Execution

A phased implementation approach was adopted to ensure a smooth transition. Phase one centered on building the new enclave and decommissioning the previous, non-compliant solution within 120 days. Phase two focused on user training and advancing towards CMMC compliance, with a target completion date six months later.

Our project team comprised experts in project engineering, security engineering, project management, and CONOPs development. Throughout the process, we maintained open communication with ZYX Corp. through weekly meetings and detailed progress reports. Strong executive sponsorship was instrumental in overcoming challenges and ensuring project success.

Several obstacles were encountered during implementation, including unexpected vendor software limitations, limited client IT resources, and the need to address preconceived notions about enclave solutions. Through effective project management, risk mitigation strategies, and close collaboration with the client, these challenges were successfully overcome.

Results and Benefits

The successful implementation of the Azure GCCH enclave yielded significant benefits for ZYX Corp.. The project was completed on time and under budget, resulting in cost savings and avoiding the expense of renewing the previous enclave license. Moreover, the new enclave provided a solid foundation for meeting 800-171 compliance requirements, enabling ZYX Corp. to retain the trust of DoD customers.

By establishing a secure and compliant IT environment, ZYX Corp. has positioned itself for long-term success in the government contracting market. While the full return on investment will materialize over time, the ability to retain existing customers and pursue new opportunities is a testament to the project's success.

Lessons Learned

This project provided valuable insights into the complexities of DoD enclave implementations. Key takeaways include the importance of thorough vendor product evaluation, maintaining open and frequent communication with clients, and proactively addressing challenges. By following these best practices, future projects can be executed more efficiently and effectively.

"Migrating part or all of an established company's IT infrastructure and operations into a secure enclave may be the most significant technical challenge a company will face. It certainly was for us. Very complicated, with many moving parts and requiring significant internal change. Huttan Holding got it done for us under budget. Their credentials, knowledge and experience with cybersecurity and 800-171 make them world-class. Their tight, hands-on, project management and transition methodology is able to deliver on all project requirements. They proved their company's core character. Very highly recommended."

–Reference Client Access Available

Huttan Holding LLC Capabilities Statement and Contact Information

Did you find this position paper of value? Here are some of our other papers.

1. IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
2. Secrets of Hiring and Firing vCISOs
3. CMMC Compliance-The New Enclave Approach
4. The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis

About the Authors:

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/