Case Study: Closing Gaps in Cybersecurity to Improve Supply Chain Resiliency

National Issues: In 2022, cybercrime complaints soared, with the FBI recording 800,000 cases and losses exceeding **$10 billion**. The National Institute of Standards and Technology (NIST) underscores the need for robust cybersecurity measures to combat these threats. As cyber threats continue to escalate, businesses of all sizes face a critical imperative to adopt **a proactive defense**. They bear the responsibility to safeguard their data and to protect that of their clients. This requires significant financial investments in technology and cybersecurity expertise. Due to the evolving digital landscape, such investments are difficult but essential for the survival and success of businesses, especially those participating as third-party suppliers.

The NIST Information Technology Laboratory defines a third-party as an external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, with or without a contractual relationship with the first-party organization.

Data reveals that more than half of global organizations have suffered data breaches originating from third-party vendors, underscoring the necessity for U.S. corporations to prioritize this risk. Compounded by the anticipated global cybersecurity labor shortage, which is projected to reach 3.9 million jobs, will make addressing cyber issues even more challenging. Closing the cyber gap requires a 62% expansion in the cybersecurity workforce, both internally and externally, for organizations.

Amidst the increasing cybersecurity demands placed on suppliers and the scarcity of cybersecurity professionals, **supply chain vendors must take decisive action to remove barriers**. Only by doing so can they ensure their continued participation in the critical national supply chain ecosystem.

Project Challenges: A U.S.-based non-profit organization encountered numerous obstacles while striving to bolster cybersecurity maturity and workforce readiness among its members who play pivotal roles in the national supply chain. These issues were prompted as mentioned above by the escalating third-party risk mandates arising from corporate and federal procurement entities. The following challenges were encountered by the organization:

- Lacked expertise in cybersecurity
- Limited knowledge of third-party barriers
- Not configured to train in cybersecurity
- No established cyber standard for its members

Solution: The **CyberReadyMBE®** program was implemented to offer cybersecurity awareness and training that included fundamentals, standards, and requirements for doing business with various sectors related to cybersecurity requirements.

Approach: As an experienced cybersecurity consulting organization with experts from various sectors, IWS analyzed the current state of the organization members such as size, sectors, and cyber protocols required based on NAICS codes. Roundtable discussions were held to determine key performance indicators and outcomes. Based on industry sectors, aligned training, practices, and workshops were provided allowing the members to train, skill up, and implement cybersecurity practices to meet cyber readiness level one as suggested by the U.S. DoD which serves as an entry-level readiness for most corporations.

Results: The implementation of the CyberReady program yielded significant success for the organization such as awareness, outreach to the entire national membership, and recruiting of over 1,000 members, with a percentage participating in workforce development training and cyber assessments, and many now having an enhanced cyber posture meeting the U.S. DoD

All Rights Reserved
Industry Workforce Solutions
9800 Connecticut Drive
Crown Point, Indiana 46307

requirements. Additionally, certificate and designation pathways were provided giving tangible recognition for the members, signifying their commitment to cybersecurity excellence and compliance. The initiative facilitated the swift onboarding of member companies into corporate supply chains and opened doors to increased government contracts, fostering a more inclusive and secure business ecosystem.

By offering the CyberReady program to its members the non-profit was able to tackle critical concerns facing businesses with the following outcomes:

- Advance the mission of cyber readiness within the organization
- Educated member companies on cyber readiness imperatives
- Ensured compliance with the latest cyber policies and practices
- Assisted in the identification and mitigation of cybersecurity vulnerabilities
- Empowered businesses to stand out in the competitive marketplace
- Unveiled novel opportunities through enhanced cyber capabilities

For more information contact us at **info@industryworkforcesolutions.com.**

All Rights Reserved
Industry Workforce Solutions
9800 Connecticut Drive
Crown Point, Indiana 46307