Building Cyber-Resilience in Bangladesh: A Case Study on the DASPiB Project

Daffodil University · TEIN · Asi@Connect · European Union · BdREN

Background

The DASPiB project was conceived against the backdrop of a rapidly evolving cyber landscape, with the goal to create a pool of skilled cybersecurity professionals who can address emerging cyber threats and secure the nation's cyber assets. Recognizing the lack of adequately trained personnel in this space, DASPiB was designed to equip trainers and participants with the necessary skills and knowledge to secure their cyberspace in Bangladesh. In addition, the project aimed to prepare individuals for internationally recognized certifications and develop a pool of cyber security professionals who could contribute towards building a safer, digitally enabled Bangladesh. The Developing Advanced Security Professional in Bangladesh (DASPiB) project, executed by Daffodil International University Bangladesh (DIU) and Bangladesh Research and Education Network (BdREN), was funded by Asi@Connect and the European Union.

Objectives

The DASPiB project targeted several objectives that address the development of cyber security knowledge and skills within the nation. The main objectives were to:

• Create cyber security awareness.

• Build a countrywide pool of cyber security professionals.

• Generate recommendations for a national cyber security policy for research and education.

• Create certified cyber security professionals.

• Foster industry-academia collaboration on cyber security.

• Create industry-ready trainers on cyber security.

• Develop competencies for providing consultancy services to other NRENs.

• Prepare industry-ready professionals to staff Security Operations Centres (SOC) with CERTs/CSIRTs around the country.

Project Design

The project was designed with a dual focus: to cultivate a pool of advanced security professionals through the Certified Ethical Hacker (CEH) training programme, and to raise public awareness regarding secure cyber practices through the CyberSafe program.

The DASPiB project is a clear example of a strategic and well-designed initiative that directly addresses the urgent need for advanced cybersecurity professionals and public education on secure cyber practices in Bangladesh. By focusing on these crucial areas, the project has made significant strides in strengthening the nation's cyber-resilience.

Project Activities

The DASPiB project was a multifaceted initiative consisting of five distinct components. However, the Certified Ethical Hacker (CEH) and CyberSafe training programs were the major activities undertaken.

· Activity-1

Certified Ethical Hacker (CEH) Training:

• The 12-day CEH program was an intensive course aimed at creating cybersecurity professionals.

• Training was conducted in five regions across Bangladesh, both online and offline, to ensure a broad reach.

• 86 trainers from various backgrounds were trained on the techniques employed by hackers to exploit network vulnerabilities and how to mitigate such threats.

Certified Ethical Hacker Training

· Activity-2
CyberSafe Workshop:
• The 4-day CyberSafe program was designed to promote cyber awareness among the general populace.
• Both online and offline trainings were conducted across five regions.
• The programme trained 300 participants on the secure use of cyberspace and how to protect their digital assets.

Cyber Safe Workshop

To facilitate the learning process, trainees were provided with logistical support including training kits, meals, and transportation. All sessions were conducted by highly skilled trainers.

Outcomes

The outcomes of the DASPiB project were multifaceted:
• The CEH and CyberSafe programs successfully trained 86 trainers and 300 participants, respectively.
• The broad reach of the training sessions, both online and offline, across five regions ensured widespread impact.
• The project has developed a pool of capable cybersecurity practitioners, significantly improving the cyber defence landscape of Bangladesh.

Impacts

The DASPiB project had far-reaching impacts:
• The creation of skilled cybersecurity professionals significantly bolstered the defence against digital threats.
• The CyberSafe program improved cyber awareness among everyday internet users, enhancing their ability to safeguard their digital identities.
• The trained professionals brought their knowledge to various organizations, strengthening institutional cyber defence mechanisms.
• The project has considerably boosted the cybersecurity landscape of Bangladesh.

Technology Transfer

The DASPiB project played a crucial role in the practical application of theoretical cybersecurity knowledge, empowering participants with real-world skills to combat cyber threats.

Conclusion

The DASPiB project marks a significant step in improving Bangladesh's cybersecurity preparedness. By delivering targeted, effective, and inclusive training across the country, the project has enriched the pool of cybersecurity professionals, fostered increased awareness, and laid the foundation for stronger industry-academy collaboration. It serves as a promising model for similar initiatives in the future, with lessons learned from its implementation contributing to the continuous improvement of cybersecurity training and preparedness in Bangladesh and beyond..