Developing and Implementing a CIRT Team

Nan Poulios
Easy I, Inc

Abstract

This session considers the necessary steps to build, implement, and train a successful computer incident response team (CIRT). We will discuss the necessary requirements for building the team, the policies and procedures of the organization, the responsibilities of the team, as well as the training of the team. We will follow a standard practice example starting with the authority for establishing a team including an organization's responsibilities for compliance with FISMA, NIST guidelines as well as others including HIPAA, GLBA, and SB1386 etc. We will examine how we select the members of a team, how we determine the individual roles and duties of CIRT team members as well as the duties of the team as whole. The standard practice will explore training needs and the use of practical exercises to prepare the team.

We will also illustrate the procedures that the CIRT team will follow when responding to an incident including on call rotation, the identification of an incident, the classification of the incident, and the escalation process. Also covered will be methodologies for the investigative process that include maintaining an investigative toolkit, evidence collection, preserving evidence, transporting evidence, the retention period, final reporting, and resolution of the incident. We will end the session with a discussion of when your in-house CIRT team should escalate the investigation to professional investigators or law enforcement.

Biography

Nan is a CISSP, CISM and holds an MA degree from Wayne State University. She has been a security consultant, instructor, standards specialist, corporate communications consultant, and project manager in information protection and security for large and small-scale computer networks for the last fifteen years. Nan has successfully delivered and managed security solutions in the financial, pharmaceutical, insurance and public utility industries, including many Fortune 500 organizations.

Currently, Nan is a Senior Training Consultant for Easy i, an international business that helps organizations to plan and implement effective information security awareness and training solutions. She is also an Adjunct Instructor for Norwich University and Walsh College. Both institutions are nationally recognized Centers of Excellence by the NSA. She has designed and taught a master's level course entitled, "Implementing a Security Program" which focuses on communicating security awareness topics throughout the corporate environment and developing an information security strategy in support of the business strategy and functions. Nan has an undergraduate degree in English and

Communicative Arts and Sciences as well as masters degree from Wayne State University.