SMALL BUSINESS
KNOWLEDGE AND
TRAINING PORTAL

TSBDC.org

AMERICA'S SBDC TENNESSEE

INCIDENT RESPONSE FROM AN I.T. PERSPECTIVE

LESSON TOPICS

1. Defining an Incident Response Plan

An Incident Response Plan is how IT professionals are going to minimize damage done by a cyber incident. This plan will have the detailed step-by-step actions your team will take to mitigate and stop the spread of a cyber attack. The plan should be well documented and written down

2. What Should it Include

The incident response plan should cover small incidents all the way up to a large cyber attack incident.

Team members and their roles should be clearly defined within this plan.

Maybe the most important part of creating an incident response plan, would be to rehearse and practice all the scenarios within before there is actually an incident in the workplace.

3. Where to Begin

The hardest part of creating the plan can be where to begin or how to organize the information. Templates and outlines are available at:

www.cisa.gov

www.nist.gov

These websites provide solid clear documentation to follow, so that you are not having to start from scratch.