Incident Response Plan

Create policies

- [ ] Set guidelines for communication, including who should be alerted and when
- [ ] Decide how you will monitor events and how you will report them
- [ ] Set dates to have fire drills and put your plan to the test

Identify attack and severity level

- [ ] Where did the attack happen
- [ ] Who was affected by the attack
- [ ] What data and systems were involved in the attack
- [ ] Document all of your findings
- [ ] Notify the appropriate contacts

Contain the threat

- [ ] Decide if the attack afftected the local computer, system or network
- [ ] Decide if it's better to shut down the network or continue to run and monitor

Get rid of the threat

- [ ] Run antivirus software
- [ ] Uninstall necessary software and hardware

Reflection

- [ ] Reflect on what happened and how the situation was handled
- [ ] Identify if changes need to be made to the plan for the future
- [ ] Note what went right and what went wrong
- [ ] Identify assets, key users and recovery team
- [ ] Amend policies in place to prevent future attacks

888.955.9706
www.mcmtsg.com