Team: Team 15

Inject Number: 34

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 02 Feb 2019 21:55:00 +0000

From: IT Director

To: IT/IS Security Team

Subject: 3.6.1 Incident Response - APT Attack

We have been advised this morning by the FBI that our internal network has been infiltrated in the general manner of an APT attack.
We need to step up our detection methods to insure that we do not have a breach of our intellectual property and confidential data.

We need to be prepared with an incident handling plan. IAW NIST 800-171 Section 3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

REQUIRED: Please develop and incident handling policy in the event that we do have a breach. What technical steps and tasks will we take if a breach is detected.

Thank you.

IT Director