Fox School of Business
TEMPLE UNIVERSITY®

Cyber Security Preparedness

- Is the organization prepared for the upcoming attack? Items to Cover:
  - Cybersecurity – Intrusion Management Policies
  - Data Collection
  - Talent
  - Appropriate Authority
  - Existing Assets

Policies

Fox School of Business
TEMPLE UNIVERSITY®

- Cybersecurity – Intrusion Management Policies
  - Does the policy differentiate from Incident Response planning and Disaster Planning
  - Does the policy provide the appropriate authority to incident manager to make decisions
  - Does the policy call for appropriate training and budget for the team.
  - Etc.

Preparation - Data Collection

Organization must have sufficient detection & monitoring capabilities to detect incidents in a timely manner

Proactive Detection includes:

- Network Intrusion Detection/Prevention System (NIDS/NIPS)
- Host Intrusion Detection/Prevention System (HIDS/HIPS)
- Antivirus, Endpoint Security Suite
- Security Information and Event Management (Logs)
- Vulnerability/audit testing
- System Baselines, Sniffer
- Centralized Incident Management System
- Input: Server, system logs
- Coordinates & co-relates logs from many systems
- Tracks status of incidents to closure

Reactive Detection: Reports of unusual or suspicious activity

Team – Skills

Fox School of Business
TEMPLE UNIVERSITY®

Is the Incident Response team – internal / external?

- Internal
  - Are the team members over allocated
  - Are the team members appropriately trained and skilled
  - Etc
- External
  - Does the organization rely on external service providers to perform any intrusion management and analysis
  - Are there appropriate contracts in place
  - Is the external team fully aware of Company policies
  - Are there appropriate contacts with local law enforcement

Assets

Fox School of Business
TEMPLE UNIVERSITY®

Has the organization kept an accurate inventory of their assets

Are they asset owners and stake holders identified

Are appropriate contracts and service levels in place with the vendors of the IT asset.