HOW TO KNOW WHAT TO PROTECT

Do you know what organizational assets you need to protect? Is it only your IT assets? Are you unclear where to start?

These are the first questions in developing an asset protection strategy. All that is needed is an understanding of your business and some time to develop an outline.

The Carnegie Mellon Risk Management Methodology (RMM) (which the NCSS CARES questionnaire is based upon) lists asset definition and management as the first step in a cyber secure business strategy. It is recommended you identify the organizational assets (people, information, technology, facilities) and assign responsibility of those assets in order to protect them appropriately.

Once organizational assets are defined, the next step is to define the relationship between these assets and the high value services they support. It requires a process be established that examines and validates this relationship through periodic reviews. Lastly, it requires your organization to maintain and sustain an inventory of these assets and high value services. It is important to keep this information up to date and modified when events change.

RESOURCES NEEDED:

- Inventory of Organizational People, Data, Technology, Facilities
- Listing of High Value Services
- Mapping
- Inventory Update Plan
- Continuity Plan

STEP-BY-STEP INSTRUCTIONS:

1. Inventory – create an inventory of your people – not just your employees, but your suppliers and partners; the data you need to run your business; the technology assets you need (computers, servers – the entire infrastructure); and the facilities needed to house and operate your business.

2. Listing of High Value Services – create a list of high value services that keep your business functioning – logistics, financial, service delivery, assembly, manufacturing. Define what are the key services you need – those services that if lost, delayed or compromised would impact your business.

3. Mapping – create a mapping of people, data, technology and facilities to the high value services they support. Define the relationship between these assets and the high value services. Validate the relationship through periodic reviews. As an example, if the supplier for your medical equipment changes, and this supplier has been identified as key personnel, have you updated your mapping relationships? Did you review the contract with the new medical supplier to determine if anything has changed that would affect your service delivery? Leveraging your people to take responsibility for certain high value services and keeping the critical information current is key to protecting your assets.

4. Inventory Update Plan – a plan is only useful if it is kept current and up-to-date. Schedule an annual inventory and mapping exercise to ensure that the protection mechanisms you employ support valid assets. A good rule of thumb – once a year.

5. Continuity Plan – A sound business strategy includes continuity plans. For all your high value services that depend on critical people, data, technology and facilities, you will need a contingency plan in place in the event any of these assets is compromised. See our "How-to-Guide" to develop a Continuity Plan.

COMMENTS/SUGGESTIONS/FEEDBACK ARE ALWAYS WELCOME AT WEB@THENCSS.ORG