HEXAGON | US FEDERAL

TABLETOP EXERCISE (TTX) PARTICIPANT GUIDE

October 5th, 2021

0830 – 1600

Hexagon US Federal
October 5th, 2021

CyberProtex
got cyber? ®

HEXAGON | US FEDERAL

AGENDA

830	Introductions
835	Roll Call
845	Emergency Contact information
	Why TTX?
900	Implementing Risk Management
945	Break
1000	Exercise - Roles and Responsibilities
1015	Recommendations and Mitigations
1100	Break
1115	Exercise - Ransomware Outbreak
	Recommendations and Mitigations
1200	Lunch Break
1300	Welcome Back!
1330	Exercise - Datacenter Problems
	Recommendations and Mitigations
1415	Break
1430	Exercise - Data Loss Prevention and Insider Threat
	Recommendations and Mitigations
1520	Break
1430	Exercise - M365 - GCC Enterprise Continuity and Compliance
	Recommendations and Mitigations
1600	Path Forward

CyberProtex
got cyber? ®

Introduction

Cyber Resilience is the ability of the enterprise to adapt to cyber-attacks and emergency events that impact the confidentiality, integrity, and availability (CIA) of business operations.

Malicious actors, from state-sponsored players to criminal enterprises, will exploit vulnerabilities as well as crisis situations to attack critical infrastructure and crucial businesses. Building a culture of relationships between stakeholders, IT professionals, continuity managers, and others within an organization, public or private, and across an industry will improve operational resilience.

To strengthen the flow of information between professionals attending and to improve operational resilience, CyberProtex will conduct a tabletop exercise to examine processes and procedures associated with cyber resiliency.

The exercise is designed to facilitate communication and response among professionals following a cyber-attack of an injection of ransomware. The event causes several critical assets to be inaccessible.

Concept of Operations (CONOPS)

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions they would take in response to an emergency. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting a large medical center. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives.

If you have any questions pertaining to the training, please email training@cyberprotex.com.

What is a Tabletop Exercise (TTX)?

A tabletop exercise (TTX) is a low-cost tool that allows key stakeholders involved in the planning and implementation of Cyber Resiliency management plans for planned special events to test the plan through a facilitated scenario-based discussion and to identify gaps.

What is the Purpose of the TTX?

- To review Cyber Resiliency, incident response and risk management plans
  OR
- To improve multi-discipline response to incidents.
- To test assumptions made during the development of the risk management plan.
- To simulate communication exchanges that will be a necessary component of the day of event operations plan incident response

Why Exercise using TTX?

- Proactive planning tool – testing cyber resiliency management plans the day of the event is too late
- To establish interagency relationships prior to the event

- To develop a common understanding of each stakeholder’s role during a planned special event and the resources they have available for use
- To develop common, unified goals and objectives
- To test the cyber resiliency plan that has been developed to ensure that it addresses a range of possible scenarios

Key Roles - Facilitator, Note Takers and Key Participants:

Facilitator - Ben McGee

- Someone who is knowledgeable, but is not an exercise “player”
- Needs to set clear goals and objectives
- Prepared to deal with group dynamics
- Ability to identify and avoid tangents to keep discussion on track

Note Taker - Melissa Bowen / Michael Sedlacek

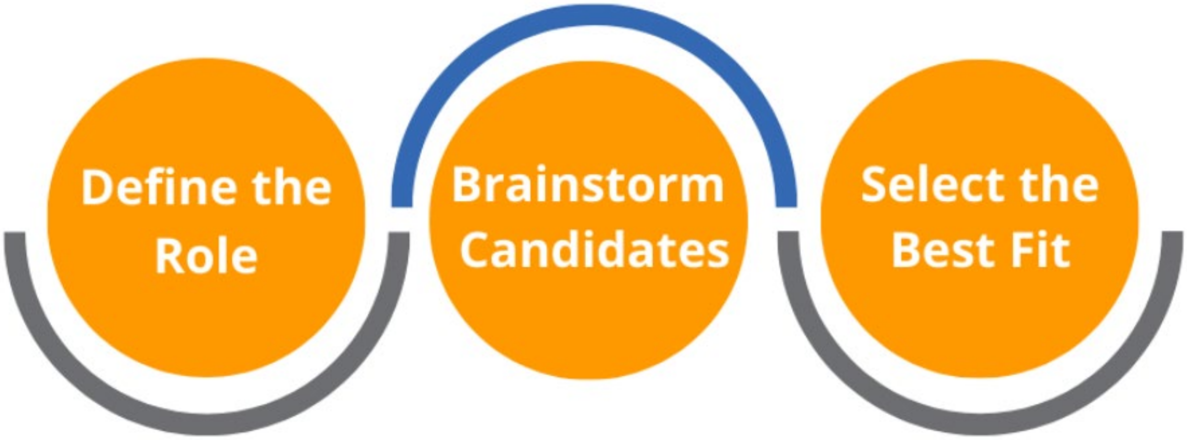
- Knowledgeable and has a clear understanding of the cyber resiliency plans for this planned special event/or has knowledge of incident management but not involved in the management of the event
- Responsible for observing discussion and taking clear notes
- Responsible for recounting observations during the review process

Key Participants - Hexagon US Federal Employees

***What* is the Purpose of THIS TTX for Hexagon US Federal?**

- Review standard operating procedures of participating departments
- Identify and address issues/concerns regarding:
    - Incident Response - Ransomware
    - Datacenter - Fire, Power, Backup and Resiliency
    - Enterprise Application Failure - M365, Deltek - Costpoint, Salesforce
    - Insider Threat - Disgruntled Employee, Information Spillage, Active Shooter
- Discuss contingency plans for possible unexpected occurrences
- To discuss implementation of cyber resiliency management plan

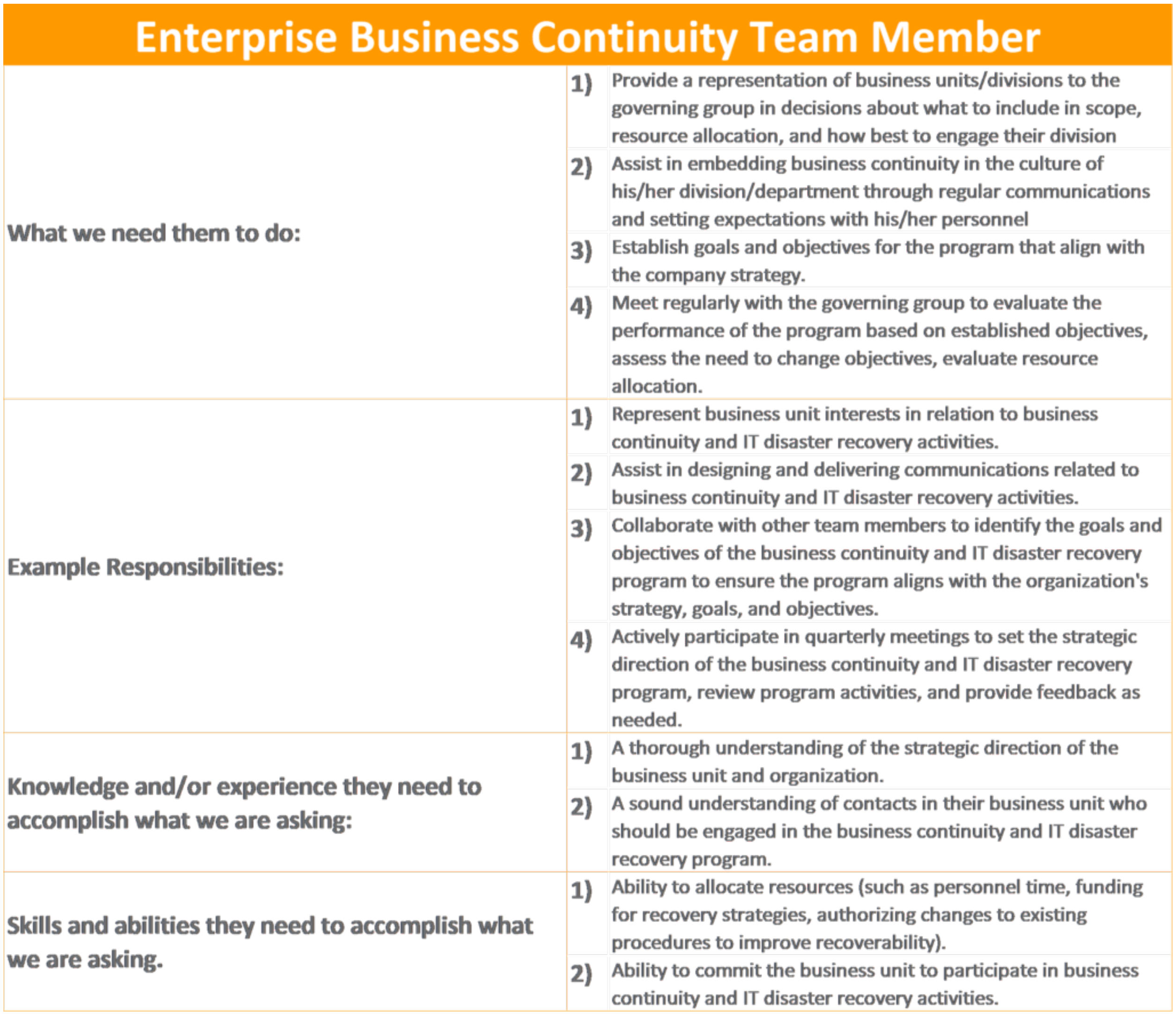
Roles and Responsibilities



Define the Role

Brainstorm Candidates

Select the Best Fit



Enterprise Business Continuity Team Member		
What we need them to do:	**1)**	Provide a representation of business units/divisions to the governing group in decisions about what to include in scope, resource allocation, and how best to engage their division
	2)	Assist in embedding business continuity in the culture of his/her division/department through regular communications and setting expectations with his/her personnel
	3)	Establish goals and objectives for the program that align with the company strategy.
	4)	Meet regularly with the governing group to evaluate the performance of the program based on established objectives, assess the need to change objectives, evaluate resource allocation.
Example Responsibilities:	**1)**	Represent business unit interests in relation to business continuity and IT disaster recovery activities.
	2)	Assist in designing and delivering communications related to business continuity and IT disaster recovery activities.
	3)	Collaborate with other team members to identify the goals and objectives of the business continuity and IT disaster recovery program to ensure the program aligns with the organization's strategy, goals, and objectives.
	4)	Actively participate in quarterly meetings to set the strategic direction of the business continuity and IT disaster recovery program, review program activities, and provide feedback as needed.
Knowledge and/or experience they need to accomplish what we are asking:	**1)**	A thorough understanding of the strategic direction of the business unit and organization.
	2)	A sound understanding of contacts in their business unit who should be engaged in the business continuity and IT disaster recovery program.
Skills and abilities they need to accomplish what we are asking.	**1)**	Ability to allocate resources (such as personnel time, funding for recovery strategies, authorizing changes to existing procedures to improve recoverability).
	2)	Ability to commit the business unit to participate in business continuity and IT disaster recovery activities.

Exercise - Roles and Responsibilities

Roles and Responsibilities – Enterprise Level

Come up with a list of Five Key Roles within the Organization related to Disaster Recovery?

What are the Responsibilities of each role?

Who do you think should be in each of these Roles?

ENTERPRISE ROLES			
Name	Services Supported	Department	Location

Roles and Responsibilities – Department Level

Come up with a list of Five Key Roles within the Department related to Disaster Recovery?

What are the Responsibilities of each role?

Who do you think should be in each of these Roles?

DEPARTMENT ROLES			
Name	Services Supported	Department	Location

Exercise - Asset Management

Number of Assets	
People:	
Information:	
Technology:	
Facilities:	
Total Assets:	

CRITICAL ASSET PROFILE					
Name	**Services Supported**	**Department**	**Location**	**Data Owner**	**Data Custodian**

Threats and Vulnerabilities

Identify threats and their level. A threat is anything that might exploit a vulnerability to breach your security and cause harm to your assets. Here are a few common types of threats:

Natural disasters. Floods, hurricanes, earthquakes, fire and other natural disasters can destroy much more than a hacker. You can lose not only data, but the servers and appliances as well. When deciding where to house your servers, think about the chances of a natural disaster. For instance, don’t put your server room on the first floor if your area has a high risk of floods.

System failure. The likelihood of system failure depends on the quality of your computer for relatively new,high-quality equipment, the chance of system failure is low. But if the equipment is old or from a “no-name”vendor, the chance of failure is much higher. Therefore, it’s wise to buy high-quality equipment, or at least equipment with good support.

Accidental human interference. This threat is always high, no matter what business you are in. Anyone canmake mistakes such as accidentally deleting important files, clicking on malware links, or accidentally physical damaging a piece of equipment. Therefore, you should regularly back up your data, including system settings, ACLs and other configuration information, and carefully track all changes to critical systems.

Malicious humans. There are three types of malicious behavior:

- **Interference** is when somebody causes damage to your business by deleting data, engineering a distributed denial of service (DDOS) against your website, physically stealing a computer or server, and so on.

- **Interception** is classic hacking, where they steal your data.

- **Impersonation** is misuse of someone else’s credentials, which are often acquired through social engineering attacks or brute-force attacks or purchased on the dark web.

Exercise – Threats and Vulnerabilities

THREATS AND VULNERABILITIES			
Name	**Services Effected**	**Department**	**Location**

Risk Assessments

What is a risk assessment?

With threats to sensitive data growing in both number and sophistication every day, organizations cannot afford a scattershot approach to security. Instead, they need to focus their limited IT budgets and resources on the specific vulnerabilities in their unique security posture.

To do this, they need to identify, analyze, and prioritize the risks to the confidentiality, integrity or availability of their data or information systems, based on both the likelihood of the event and the level of impact it would haveon the business. This process is called IT risk assessment.

Risk assessment is primarily a business concept, and it is all about money. You must first think about how your organization makes money, how employees and assets affect the profitability of the business, and what risks could result in large monetary losses for the company. After that, you should think about how you could enhance your IT infrastructure to reduce the risks that could lead to the largest financial losses to organization.

Basic risk assessment involves only three factors: the importance of the assets at risk, how critical the threat is, and how vulnerable the system is to that threat. Using those factors, you can assess the risk—the likelihood of moneyloss by your organization. Although risk assessment is about logical constructs, not numbers, it is useful to represent it as a formula:

Risk = Asset X Threat X Vulnerability

Although risk is represented here as a mathematical formula, it is not about numbers; it is a logical construct. Forexample, suppose you want to assess the risk associated with the threat of hackers compromising a particular system. If your network is very vulnerable (perhaps because you have no firewall and no antivirus solution), and the asset is critical, your risk is high. However, if you have good perimeter defenses and your vulnerability is low, and even though the asset is still critical, your risk will be medium.

When looking at risk, it's good to keep several questions in mind. Raising these questions helps ensure that the risk analysis team and senior management know what is important. Team members must ask the following:

- **What event could occur (threat event)?**
- **What could be the potential impact (risk)?**
- **How often could it happen (frequency)?**
- **What level of confidence do we have in the answers to the first three questions (certainty)?**

A lot of this information is gathered through internal surveys, interviews, or workshops. Viewing threats with these questions in mind helps the team focus on the tasks at hand and assists in making the decisions more accurate and relevant.

Why do you need IT risk assessment?

IT risk assessment should be the foundation of your IT security strategy to understand what events can affect your organization in a negative way and what security gaps pose a threat to your critical information, so you can make better security decisions and take smarter proactive measures.

IT risk assessment helps you determine the vulnerabilities in information systems and the broader IT environment, assess the likelihood that a risky event will occur, and rank risks based on the risk estimate combined with the level of impact that it would cause if it occurs.

IT risk assessment is required by many compliance regulations. For instance, if your organization must comply with CMMC, then information security risk assessment is a must-have for your organization to minimize the risk of noncompliance and huge fines.

Document the Results. The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and so on. For each threat,the report should describe the corresponding vulnerabilities, the assets at risk, the impact to your IT infrastructure,the likelihood of occurrence and the control recommendations. Here is a very simple example:

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air conditioning systems is ten years old High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost
Malicious human (interference) — DDOS attack High	Firewall is configured properly and has good DDOS mitigation Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall
Natural disasters — Flooding High	Server room is on the 3rd floor Low	Servers Critical	All services will be unavailable Critical	Low Last flood in the area happened 10 years ago	Low	No action needed
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup Low	Medium	Low	Continue monitoring permissions changes, privileged users, and backups

Scenario – Incident Response

An attack is unleashed from unknown hackers and all computers at Hexagon US Federal have become unusable. You can still authenticate to the domain, but all critical systems files and applications are encrypted and unusable.

Duration: The following exercise will take you through the first minutes of the incident.

Please make notes of your group's discussion of each of the exercises for questions and answers during the debriefing of each stage. Assign one person at each table to be the speaker for the table.

Exercise: Unknown Inject Date/Time: October 5th, 2021, From: To:

RISK ASSESSMENT REPORT

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Recommendations

Scenario – Datacenter

A Fire alarm sounds. Small scent of something burning. Is it a false alarm?

Duration: The following exercises will take you through the first minutes of the incident.

Please make notes of your group's discussion of each of the exercises for questions and answers during the debriefing of each stage. Assign one person at each table to be the speaker for the table.

Exercise: Unknown	**Inject Date/Time: October 5th, 2021, From:**	**To:**

RISK ASSESSMENT REPORT

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Recommendations

Scenario – Insider Threat

You have been receiving threats at your facility for multiple weeks, and to date nothing has happened. You have notified law enforcement, but they have been unable to identify a suspect.

Duration: The following exercises will take you through the first minutes of the incident.

Please make notes of your group's discussion of each of the three exercises for questions and answers during the debriefing of each stage. Assign one person at each table to be the speaker for the table.

Exercise: Unknown Inject Date/Time: October 5th, 2021, From: To:

RISK ASSESSMENT REPORT

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Recommendations

Scenario - Enterprise Applications

You use enterprise apps and programs daily. Your daily routine is about to change.

- M365 Outlook, Teams, SharePoint
- Deltek – Costpoint
- Salesforce

Duration: The following exercises will take you through the first minutes of the incident.

Please make notes of your group's discussion of each of the exercises for questions and answers during the debriefing of each stage. Assign one person at each table to be the speaker for the table.

Exercise: Unknown Inject Date/Time: October 5th, 2021, From: To:

RISK ASSESSMENT REPORT

Threat	**Vulnerability**	**Asset**	**Impact**	**Likelihood**	**Risk**	**Recommendations**

RISK ASSESSMENT REPORT

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Recommendations

PLAN OF ACTION AND MILESTONES

NAME	DESCRIPTION	PERSON RESPONSIBLE