SCANTRON®
TECHNOLOGY SOLUTIONS

Incident Response and Business Continuity Planning

SMART STARTS HERE

Agenda

- What is an Incident Response Plan
- What is a Business Continuity Plan
- Are the Plans the same
- How the Plans Work Together
- Incident Response Plan Components
- Components of a Business Continuity Plan
- Incident Response Plan or Business Continuity Plan Testing
- Incident Response or Business Continuity Plan Benefits

What is an Incident Response Plan

This plan is a play-by-play guide to help your IT Staff prepare, detect, respond to, remove and recover from a cybersecurity incident. The plan includes current processes, infrastructure and asset location information, and contact information.

Plan Goal: Identify, respond and contain a cyber attack before it gets out of hand or causes long term damage to the organization and its assets.

What is a Business Continuity Plan

This plan is the process of creating processes, systems, and recovery measures in the event the organization must deal with potential threats.

Plan Goal: Ensure the organization can continue to deliver its products or services at pre-defined acceptable levels during an incident.

Are They the Same

- Defining features differentiate each plan.
- Incident Response Plan, may be found or referenced in the Business Continuity Plan due to the over-arching goal of keeping the business functioning as intended.

How the Plans Work Together

Depending on the incident you may have to deploy both plans.

- One plan to ensure your organization’s operations continue with minimal impact to your production or customers.
- Second plan to ensure that the threat is identified, contained, eliminated and that systems get recovered.

Planning and testing will help you determine when you need one or both plans.

Incident Response Plan Components

General plan phases:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Each item should be a different phase in your plan and should have as much info regarding their section as possible.

Up-to-date, thorough information greatly increases your IT staff's response to cyber security incidents.

The Preparation Phase (IRP)

“Pre-Game” of the incident.

Information Needed:

- Assets (inventory, vulnerabilities and threats)
  - Impact to those assets if they are unavailable, become compromised, or they have a data leakage.
- Expectations: response times, resources or financial capital needs
- Notification tree
- Team identification
- Tools
- Communication requirements
- Tracking

The Identification Phase (IRP)

Tools/systems/mechanisms needed to identify a compromise.

This area will have information such as:

- Setting up monitoring
- Analyzing events
- Identification of an incident (where and what)

Examples:

- Antivirus solution notification
- SIEM (Security Information and Event Manager) Alert
- A user reports strange activities or files on system.

The Containment Phase (IRP)

Containing the incident.

This area will have information such as:

- The type of incident
- The preventative measures needed to isolate the threat

Example:

- You would not contain a ransomware attack in the same fashion you would a DDoS attack

The Eradication Phase (IRP)

Threat removal from your environment.

This area will have information such as:

- The type of incident
- The tools, steps or information need to remove the threat from the environment

Example:

- The way you deal with a compromised account versus how you deal with a rogue device on your network will be different

The Lessons Learned Phase (IRP)

Incident review and preparing for the future.

Information included:

- What happened and when
- Was the document followed
- What could be done differently to improve the situation
- What can be done to prevent this in the future

Business Continuity Plan Components

Your Business Continuity Plan should contain:

- Business impact analysis
- Identification of critical business functions and processes
- Dependencies between areas of business and functions
- Determination of acceptable down time for critical business functions
- Plan to maintain operations

Business Impact Analysis

- Identify all the functions and resources that are related that are time sensitive.
- Identify impact to both operations and financial that come from the loss of business functions and/or processes.
- Inversely be able to identify when the loss of a function or process would result in a business impact.

Critical Business Functions & Process Identification

- Items that have the greatest impact to your organization's operations.
- Gather all the information regarding your current business functions and all assets.
- Identify the risks, vulnerabilities and threats of the business functions and assets.

Determination of acceptable down time

- Make quick decisions with the least amount of impact to the organization.
- Level of acceptance identifies the incident priority level.
- Down time caused by an incident, and system recovery downtime.
- Third party relationships impacting recovery time.

Plan to Maintain Operations

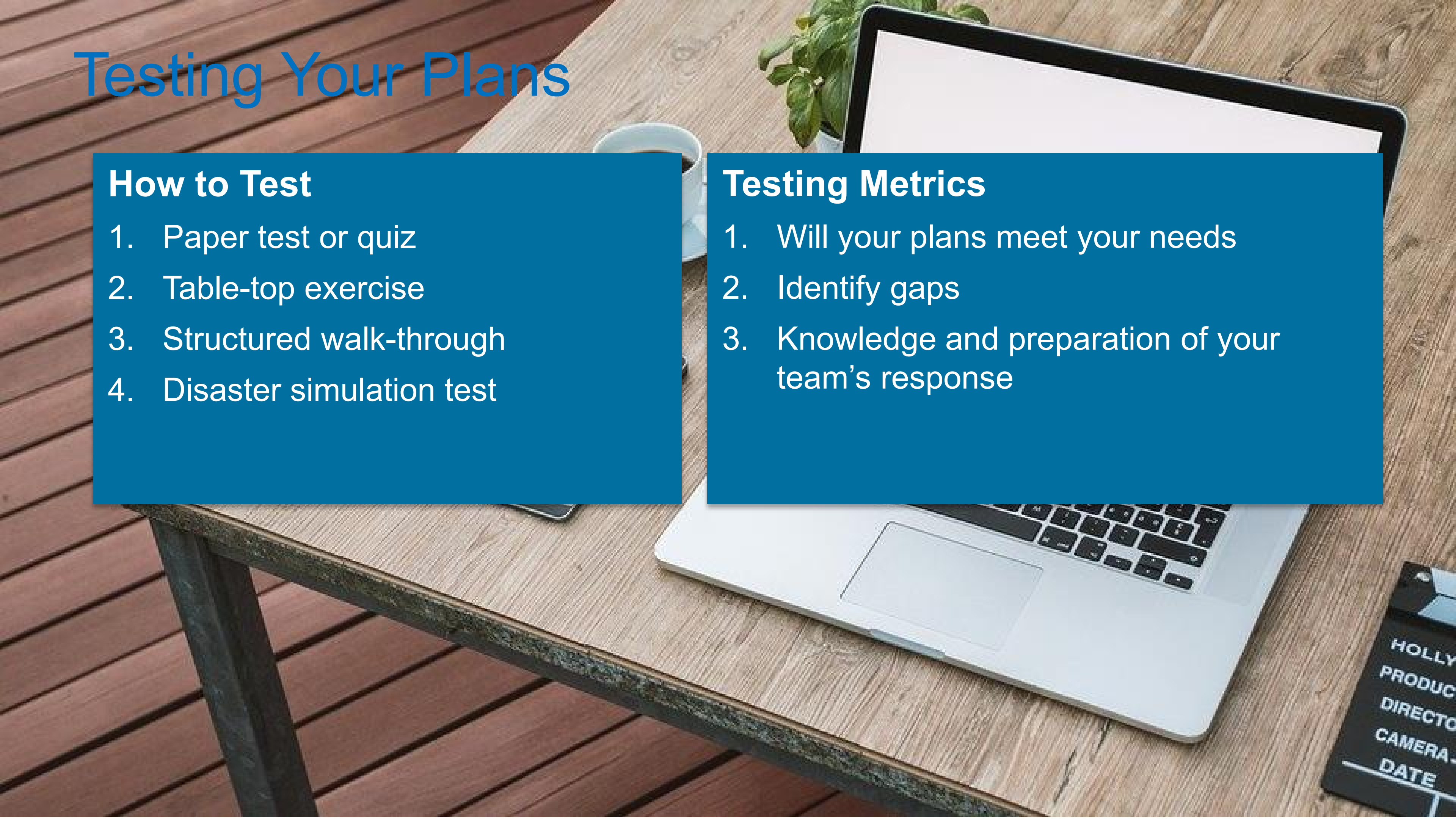
- Collect the information needed to your organization’s plan.
- Comprehensive view into your organization's operations, the risk appetite and acceptable down time.
- Include key personnel in your business units for key insights into past incidents.

Why should you test?

Plan Benefits

- Serve your customers without interruption
- Quicker recovery time for your processes and systems
- Reduced recovery cost in the event of an incident
- Build confidence and trust in your investors and customers
- Protect your organizations reputation
- Ensures compliance and industry standards are met
- Greatly mitigates risks and financial loss
- Improves security and security of assets

Testing Your Plans



How to Test

1. Paper test or quiz
2. Table-top exercise
3. Structured walk-through
4. Disaster simulation test

Testing Metrics

1. Will your plans meet your needs
2. Identify gaps
3. Knowledge and preparation of your team’s response

SMART
STARTS
HERE

SCANTRON®
TECHNOLOGY SOLUTIONS

Thank you for attending the session

Arturo Romero
arturo.romero@scantron.com

Adam Ward
adam.ward@scantron.com

Let’s connect