MAKING AN IMPACT ON U.S. MANUFACTURING

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Recovering from a Cybersecurity Incident

What to do Before and After

Patricia Toth

NIST MEP

What is Information Security?

Confidentiality

Unauthorized Access, Disclosure

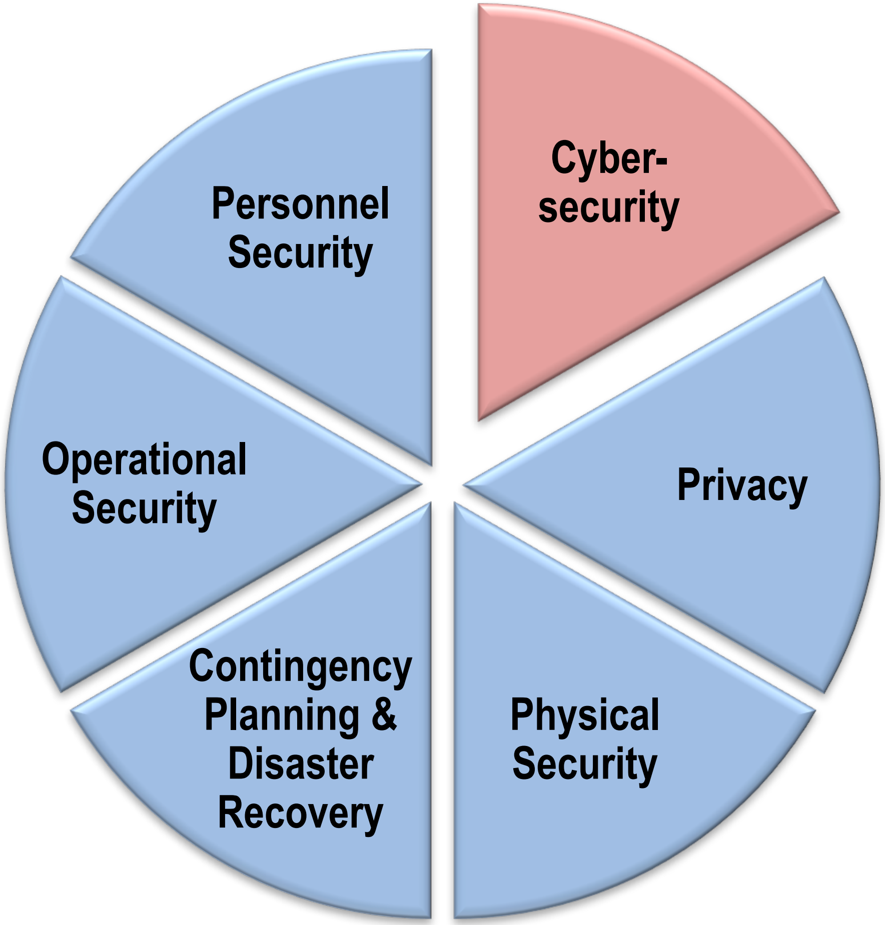
Integrity

Unauthorized Modification, Use

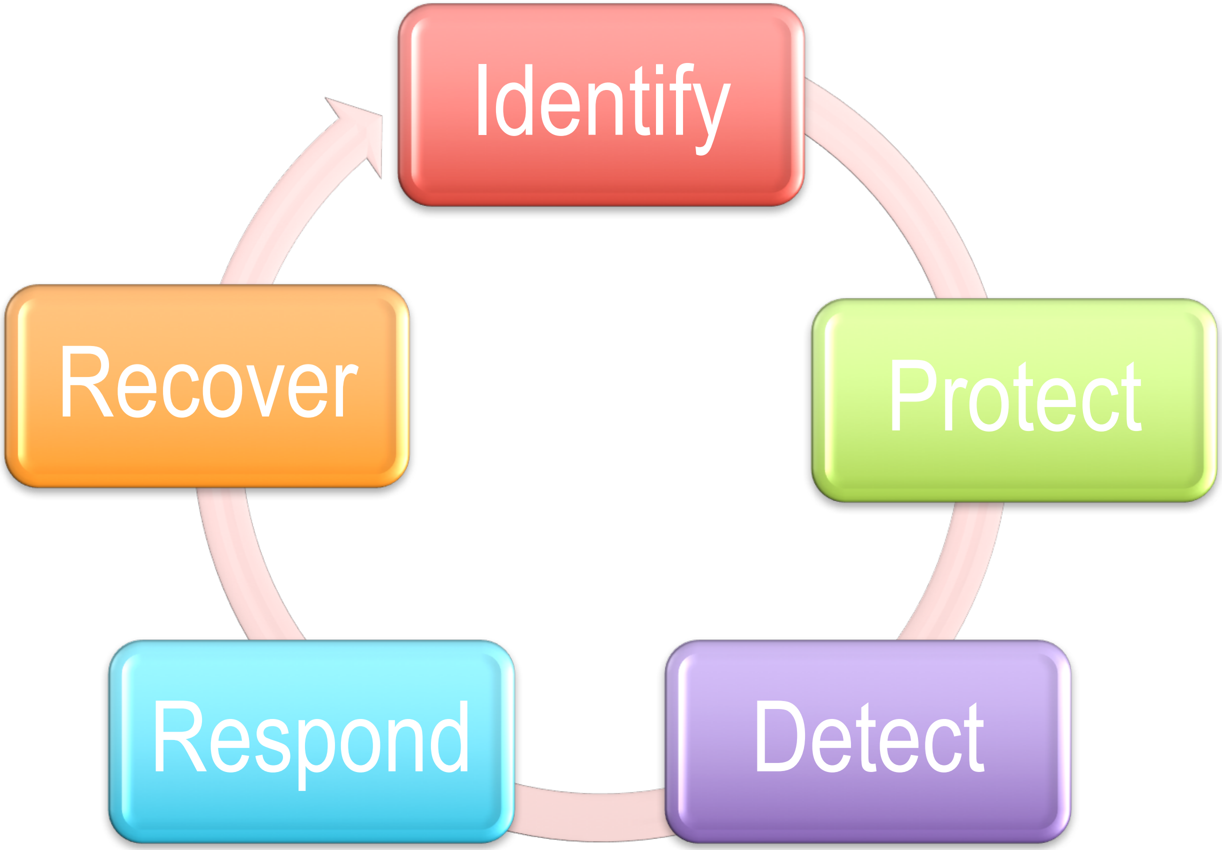
Availability

Disruption, Destruction

What is Information Security?



NIST Cybersecurity Framework



NIST SP 800-184

GUIDE FOR CYBERSECURITY EVENT RECOVERY

https://doi.org/10.6028/NIST.SP.800-184

Recover

- "The development and implementation of plans, processes and procedures for recovery and full restoration in a timely manner, of any capabilities or services that are impaired due to a cyber event"

What is a Cybersecurity Event?

- Any observable occurrence in a system or network

What is a Cybersecurity Incident?

- Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident

Actually or Potentially results in:

- Adverse Consequences
- Adverse effects
- Poses threat to

an information system or the information that system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Incident Examples

- Attempts to gain unauthorized access to a system
- Unwanted disruption or denial of service
- Unauthorized use of a system
- Changes to system HW, FW or SW characteristics without the owner's knowledge, instruction, or consent

Examples of Incidents

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

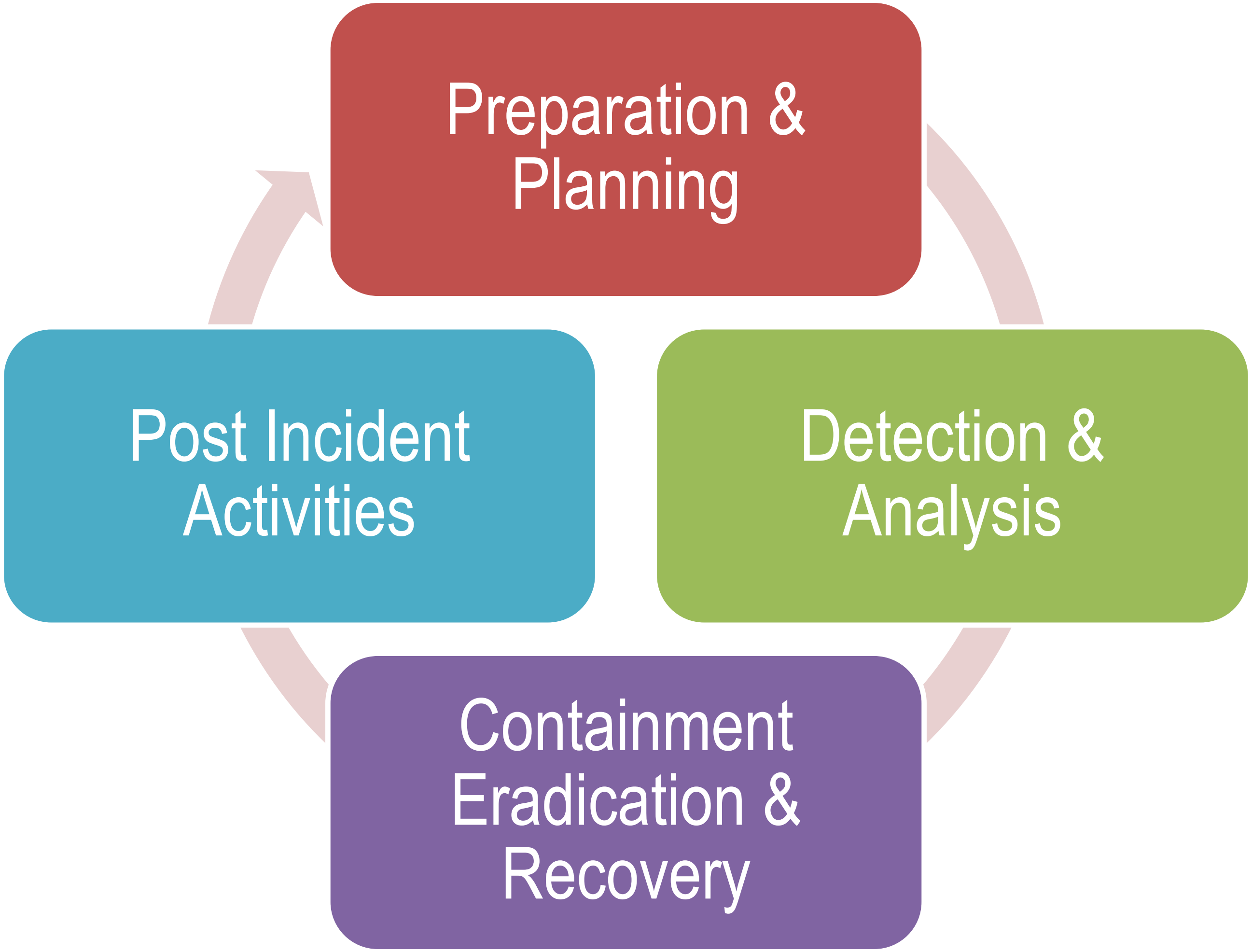
Cyber Event

- Specific cybersecurity incident or
- Set of related cybersecurity incidents that result in successful compromise of an information system

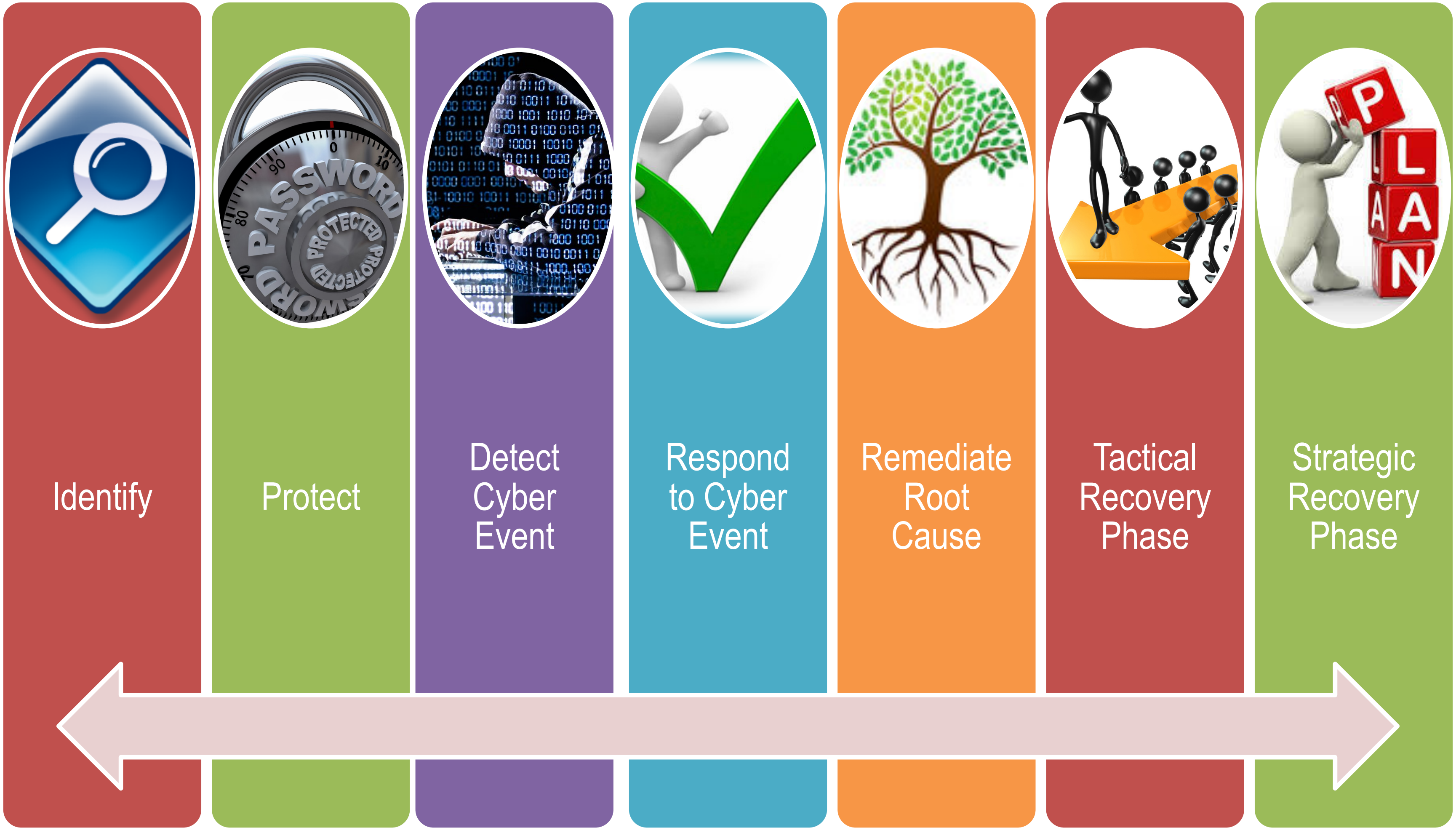
Recovering

- Simple
  - Sys Admin restores from backup
- Complex
  - People
  - Processes
  - Technologies

Incident Response Lifecycle



NIST Cybersecurity Framework



Identify

Protect

Detect Cyber Event

Respond to Cyber Event

Remediate Root Cause

Tactical Recovery Phase

Strategic Recovery Phase

Prepare & Plan

- Prepare for resilience
- Plan to operate in a diminished capacity
- Restore services based on priorities

Prepare & Plan

- Identify key people
- Understand roles and responsibilities
- Create & maintain list of assets
  - People, processes, technology
  - Mission critical
- Have a plan
  - Tech and Non-Tech
- Practice Recovery

Prepare & Plan

- Conditions for Recovery
  - Who has authority to invoke
  - How personnel are notified
- Define key milestones including termination of active recovery efforts
- Adjust incident detection and response policies
- Develop Recovery communications plan
- Define Recovery communication goals, objectives and scope

Continuous Improvement

- Gather feedback
- Exercises and tests
- Post exercise debriefs
- Lessons learned
- Identify weaknesses
- Validate recovery capabilities
- Document issues

Recovery Metrics

- Understand what should be measured
- Implement processes to collect relevant data.
- What metrics are most useful?
- Activities that cannot be measured in accurate or repeatable way

Incident Damage and Cost

- Direct and indirect costs
- May be important evidence
- Costs
  - – Loss of competitive edge
  - – Legal costs
  - – Hardware, software, and labor costs
  - – Business disruption
  - – Loss of brand reputation or customer trust

Risk Assessment Improvement

- Frequency and/or scope of recovery exercises and tests
- Number of significant IT-related incidents that were not identified in risk assessment
- System dependencies accurately identified
- Identified gaps during the recovery exercises or tests that help inform and drive the improvement in the other functions of the CSF

Quality of Recovery Activities

- Number of business disruptions due to IT service incidents
- Level of customer satisfaction
- Percent of IT services meeting uptime requirements
- Percent of successful and timely restoration from backup or alternate media copies
- Number of successful recovery events

Incident Examples

- Botnets
- Phishing Attack
- Ransomware
- Information sharing

Building a Playbook

- Tactical Phase
  - – Initiation
  - – Execution
  - – Termination
- Strategic
  - – Planning and Execution
  - – Metrics
  - – Recovery plan improvement

Building a Playbook - Tactical

Tactical

People, process, and technology assets

Dependencies among these assets

Map or diagram of the dependencies

Building the Playbook - Tactical

- Categorize all assets
- Identify key people ensure they understand their roles and responsibilities
- Ensure correct underlying assumptions
- Conditions when recovery plan invoked
- Authority to invoke the plan
- How recovery personnel will be notified
- Milestones, intermediate goals, and criteria for finalizing

Building the Playbook - Tactical

- Prevent recovery from negatively affecting the incident response
- Examine the cyber event and initiate the plan for recovery
- Recovery communications plan
- Consider sharing actionable information

Building the Playbook - Tactical

- Gather feedback
- Cyber event recovery exercises and tests
- Update cyber event recovery plans, policies, and procedures
- Improve cybersecurity posture
- Vet recovery capabilities

Building the Playbook - Tactical

- Execute the tailored playbook that has been created during the cyber event
- Document issues
- Implement monitoring for events
- Monitor the artifacts and evidence found during detection and response
- Monitoring will extend into the strategic phase.

Playing the Playbook - Strategic

Perform before and during the cyber event:

- Cybersecurity improvement plan based on tactical phase results
- Execute communications plan
- Review milestones, goals, and metrics gathered throughout the tactical phase

Cyber Event Recovery Scenario

Network Breach

- Anomalous activity detected
- Stolen credentials to gain access critical business systems
- Jeopardizes trustworthiness
- PII

Illustration by Chris Gash

- Possible customer financial data stolen

Event Pre Conditions

- Set of formal recovery processes
- List of critical people, facilities, technical components, and external services
- Playbook identifies the data breach recovery team

Event Pre Conditions

- A current set of functional and security dependency maps
- Metrics including:
  - Costs
  - Lost revenue due to business downtime
  - New services to restore customers' trust
  - Accuracy of dependencies maps
  - Gaps identified in the playbook
  - Customer satisfaction
  - Service level agreements
  - Confidence level around quality of the backups
  - Quality of recovery plan and data breach playbook

Event Pre Conditions

- Resources and tested tools
- Recovery communications plan
- Periodic training and exercises

Event Tactical Recovery Phase

Initiation

Network-based communications insecure and cannot be trusted

Personal and credit card information

Find footprints

Activities in environment

Systems impacted

Entry point identified

Compromised users and administrative accounts are identified

Infrastructure systems need to be remediated

Event Tactical Recovery Phase

Initiation

Work with IR team

Meet with business owners

Start with data breach playbook

Determine last known good state of the data

Enable additional security controls

Recovery activities might alert the adversary

Work with the IR team to increase the level of monitoring and strengthen the isolation capabilities

Determine order in which systems will be restored

Recovery process is ready to begin

Identified metrics are recorded and tracked by the responsible parties

Event Tactical Recovery Phase

Execution

- Follow modified data breach recovery playbook
- Monitor and strengthen isolation capabilities
- Resources and functions restored
- Additional security controls implemented
- Not susceptible to the original system weaknesses and are ready to be restored
- Execute recovery plan

Event Tactical Recovery Phase

Execution

Track the downtime of critical systems and services

Advise management

Document any issues that arise

Notification activities

Additional recovery steps initialized

Event Tactical Recovery Phase

Termination

- Data has been restored to a known good state
- Vulnerabilities remediated
- Adversary is no longer in the environment
- End of the tactical recovery event
- Recovery team finalizes the findings, metrics, and lessons learned collected during the event

Event Strategic Recovery Phase

Planning and Execution

- Support communication teams
- Recovery teams close the loop with external entities
- Plan developed to fully correct the root causes
- IT Team implements long-term improvement plan

Event Strategic Recovery Phase

Metrics

- After-action review
- Review key milestones

Event Strategic Recovery Phase

Recovery Plan Improvement

- Team performance
- Continually improve cyber event recovery plans, policies, and procedures

Checklist of Elements Included in a Playbook

Pre-Conditions Required for Effective Recovery

- Set of formal recovery processes
- Criticality of organizational
- Functional and security dependency maps
- List of technology and recovery personnel
- Comprehensive recovery communications

Checklist of Elements Included in a Playbook

Tactical Recovery Phase - Initiation

Briefing from IR Team

Determine the criticality and impact

Formulate an approach and set of specific actions

Heighten monitoring and alerting of the network and systems

Understand the adversary's motivation

Identify the adversary's footprints

Inform all parties that the recovery activities have been initiated

Utilize all available information to create plan

Checklist of Elements Included in a Playbook

Tactical Recovery Phase – Execution

- Execute the restoration
- Restore additional business services
- Track outage time
- Document any issues that arise
- Coordinate with management
- Additional recovery steps
- Validate the restored assets are fully functional and meet the security posture

Checklist of Elements Included in a Playbook

Tactical Recovery Phase – Termination

- Criteria met
- Declare the end of the tactical recovery event
- Stand down recovery team
- Continue to monitor the infrastructure
- Finalize the metrics collected during the event

Checklist of Elements Included in a Playbook

Strategic Recovery Phase – Planning and Execution

- Support the various communication teams
- Close the loop with external entities
- Develop a plan to correct the root cause of the cyber event
- Implement changes to strengthen security posture

Checklist of Elements Included in a Playbook

Strategic Recovery Phase – Metrics

Review metrics collected

Review achievement of key milestones and assumptions that were made pre-recovery

Checklist of Elements Included in a Playbook

Strategic Recovery Phase – Recovery Plan Improvement

- Use lessons learned recovery to enhance the recovery plan

Business Emergency Plan

- https://www.ready.gov/sites/default/files/documents/files/sampleplan.pdf

Questions?

MAKING AN IMPACT ON U.S. MANUFACTURING

National Institute of
Standards and Technology
U.S. Department of Commerce

Pat Toth

Cybersecurity Program Manager

ptoth@nist.gov

301-975-5140