Measured
Trust, quantified.

# How to Start a Cyber Incident Response Plan

Small and midsize enterprises (SMEs) face an uphill battle in cybersecurity. However, what many SMEs lack in resources can be made up for with solid planning to react swiftly and confidently to cybersecurity attacks. SMEs looking to create a cyber incident response plan today benefit from a time-tested series of steps that provide a logical plan for almost any situation.

**Click here to access Measured's Broker page**

## The six key steps to create a Cyber Incident Response Plan:

### Step 1: Preparation

- Identify who will be involved in what part of a response, including outside contractors.
- Identify all IT, legal, and C-level personnel who need to make decisions.
- Train IT staff on how to respond to threats with the tools/solutions to be used. Use table-top exercises.

### Step 2: Detection and Analysis

- Set up the tools that make it possible to monitor and detect threats.
- Define the level of reaction each threat or incident warrants.
- Correctly identifying the threat vector to its root cause and alert all the affected parties (internal or external).

### Step 3: Containment

- Isolate affected systems and software from rest of infrastructure.
- Block and log unauthorized accesses, as well as sources of malware.
- Close specific ports, mail servers, and other servers or services. Change system admin passwords, update firewall settings, rotate private keys.

### Step 4: Eradication

- Eliminate all evidence of compromise and prevent threat actor from maintaining presence.
- Reimage affected systems, rebuild from sources, and replace compromised files.
- Install patches, reset passwords, and monitor for adversary responses. Maintain close monitoring.

### Step 5: Recovery

- Restore systems to normal operations, confirm functionality.
- Reconnect rebuilt/new systems to networks.
- Tighten perimeter security, implement zero trust access rules. Test systems, including security controls.
- Monitor operations for abnormal behaviors.

### Step 6: Post-Incident Activities

- Identify and address "blind spots" to ensure adequate coverage.
- Monitor for evidence of persistent adversary presence.
- Address root causes, infrastructure problems, policy issues, and update roles, responsibilities, interfaces, and authority. Identify training needs.

## Consider Customized Plans and Training Help

SMEs can always work with cybersecurity experts to create a customized cyber incident response plan. A custom plan can help an organization better identify who should take which actions.

Threat actors don't just target the IT department – they target everyone. Making everyone mindful and prepared is the best way to anticipate and prevent threats. Employee training can enable employees to be vigilant in the event of ever-changing threats to a company's cybersecurity.

Measured
801.877.9333
**measuredinsurance.com**