
# CYBER INCIDENT RESPONSE QUICK GUIDE

A practical playbook for reducing damage, downtime, and recovery costs during a cybersecurity incident.

Written By Justin Small, US Air Force (Retired)

**Prepared By**

Justin Small, US Air Force (Retired)

Cybersecurity Consultant

25+ Years of Information Technology & Cybersecurity Experience

20-Year U.S. Air Force Veteran

CompTIA Security+ Certified

Executive VP, IT & Cybersecurity Director for Diamond Self Storage Management, LLC

---

**Creative Web Solutions -**

**Helping Small Businesses Improve Their Technology and Cybersecurity**

---

# Cybersecurity Incident Response Quick Guide

What to do during the first few hours after discovering a cybersecurity incident.
This guide is designed for employees and non-technical staff to take immediate, controlled action.

### 1. Recognize the Incident

An incident may include unusual system behavior, ransomware messages, missing files, unexpected password changes, phishing emails clicked, or unauthorized access alerts.

Do NOT assume it's harmless. If something feels off, treat it as an incident.

### 2. Immediate Containment Actions

Disconnect the device from the network immediately (Wi-Fi and Ethernet).
Do NOT power off unless instructed.
Do NOT attempt to fix or troubleshoot the system.
Stop all work on the affected device.

### 3. Reporting the Incident

Report the incident immediately to IT or your security contact.
Provide clear details:
- What you saw
- When it started
- What actions were taken
- Any emails or files involved

Speed matters more than completeness at this stage.

### 4. Preserve Evidence

Do NOT delete files, emails, logs, or messages.
Do NOT clear browser history or system alerts.
Avoid further interaction with suspicious content.

Preserving evidence helps determine scope and impact.

### 5. What NOT to Do

Do NOT attempt to investigate the issue yourself.
Do NOT reinstall software or reset passwords unless directed.
Do NOT notify external parties without approval.
Do NOT continue using the affected system.

**6. First Hour Priorities**

1. Isolate affected systems
2. Report to IT/security immediately
3. Identify affected accounts or systems
4. Preserve logs and evidence
5. Follow instructions from response team

**7. Communication Rules**

Only designated personnel should communicate about the incident.
Avoid discussing the issue via email or messaging platforms unless secure channels are provided.
Do not speculate about cause or impact.

**8. Recovery Preparation**

Once IT confirms containment, follow instructions for password resets, system restoration, and return-to-service procedures.
Do not reconnect devices until cleared.

---

**About the Author**

Justin Small has more than 25 years of information technology and cybersecurity experience, including 20 years of service in the United States Air Force. He currently serves as Executive Vice President, IT and Cybersecurity Director for Diamond Self Storage Management and provides cybersecurity consulting services to small businesses and self-storage operators throughout Texas.

For additional cybersecurity resources and consulting services, visit Creative Web Solutions, http://www.texascws.com.