

# Incident Response Checklist

## Executive/Business Perspective

Responsible for critical decision making and communications.

### ASSESS DAMAGE

- How widespread is the attack? Is it ongoing?
- Do you need to pull the plug on your tools or temporarily halt support?
- Delegate triaged outreach to affected customers
- Be aware of regulations and requirements (HIPAA, GDPR, etc.)

### GET ON THE PHONE (JUST NOT WITH YOUR CLIENTS YET)

- Contact cybersecurity insurance provider and/or lawyer(s)
- Coordinate with (insurance-approved) IR provider
- Secure additional outside help/surge capacity
- Contact law enforcement (discretionary)

### GET YOUR STORY STRAIGHT

- Determine how much to share and with who
- Coordinate with team re: communication scripts/templates for both notifying and updating clients and responding to press inquiries
- Review communications with lawyer

### UTILIZE YOUR TEAM

- Use your best technical staff to stop the bleeding  
Delegate keeping the lights on to other techs
- Have non-technical staff answering phones and responding to email
- Run damage control with key affected clients

## Technical Perspective

Responsible for containment, isolation and restoration.

### LOCK DOWN YOUR ACCOUNTS AND TOOLS

- Audit for unusual tasks, scripts, policy changes, etc.
- Disable user accounts associated with abnormal/malicious behavior; terminate active sessions
- Isolate any endpoints and other accounts associated with those users
- Minimize logging into affected systems using privileged credentials
- DO NOT shut down affected systems Change all passwords
- Ensure MFA is enabled on all accounts
- Confirm AV is enabled and updated, run deep scan
- Backup log files

### LOCK DOWN AFFECTED CLIENTS

- Isolate affected client endpoints by taking them off the network
- Ensure backups are isolated/protected
- Minimize logging into affected systems using privileged credentials
- DO NOT shut down affected systems

### NEXT STEPS AFTER ISOLATION

- Triage to determine further remediation priorities
- Strongly consider bringing in incident response specialist

Disclaimer: Any actions taken need to be tailored to your unique situation and environment. We don't take responsibility for results or outcomes.