I. Establish Reliable Facts and a Way to Stay Informed

☐ **Who** is reporting the problem? How did they become aware?

☐ **What** do we know so far about what happened?
- What networks/systems are affected?
- What data/information was compromised (e.g., stolen, deleted, altered)?

☐ **When** did the breach occur?
- When did we find out about it?
- When did we begin to do something about it?
- When will we know the full scope of the problem?
- When do we estimate that the problem will be remediated?

☐ **Where** did the breach occur (what office, activity, locale, etc.)?

☐ **How** much do we know, with certainty, about how the breach occurred? The source of the attack?

☐ **How** will we stay informed of efforts to remediate the breach and restore normal service?

II. Mobilize a Response

☐ Who has the lead in directing operational response efforts? What role will your office play?

☐ Has the MS-ISAC been notified (1-866-787- 4722)?

☐ Who else should be notified at this point (e.g., citizens, business and industry, other state, local, federal officials, etc.)?

☐ Has law enforcement been notified?

☐ What expertise is on hand to work the problem? What additional help do you need? Who will provide it?

☐ What measures are needed to secure the networks/systems from further exploitation?

☐ What additional steps are needed to secure data holdings?

☐ How will the remediation efforts to limit/repair the damage and restore normal services be prioritized?

☐ What special notifications should be prepared for victims?

☐ What other actions do your breach notification laws require?

☐ What are the legal implications of the incident?

III. Communicate What You Know

☐ Here, as elsewhere, bad news does not get better with age, but remember the general rule that the first report is always wrong.

☐ Release your initial public statement as soon as you have a reasonable command of the problem and can explain what you are doing about it.

☐ Describe what you know so far about what happened and what is being done to correct it.

☐ Be prepared to explain the pre-existing cybersecurity posture and the measures that were in place to prevent events of this kind.

☐ Be prepared to explain the steps you will take to prevent future unauthorized intrusions. Start with basic cyber hygiene and the Critical Security Controls.

☐ Establish a regular cadence of updates for victims, media, and other stakeholders - including your own workforce.

Need Help?
Call the MS-ISAC
1 - 866 - 787- 4722 (24 hours)
www.cisecurity.org

National Campaign for

Cyber Hygiene

Count, Configure, Control, Patch, Repeat

COUNT
Know what's connected to and running on your networks and systems

CONFIGURE
Implement key security settings to help protect your networks and systems.

CONTROL
Permit only approved software. Limit and manage Admin privileges.

PATCH
Regularly update all apps, software, and operating systems.

REPEAT
Regularize this process to put in place basic cybersecurity hygiene for your organization.

These steps constitute a minimum standard of due care for cybersecurity!

http://www.cisecurity.org
/about/CyberCampaign2014.cfm

MS-ISAC
MULTI-STATE
Information Sharing
& Analysis Center™

Center for
Internet Security®

Mid-Atlantic Headquarters
1700 North Moore Street
Suite 2100
Arlington, VA 22209
+1 518-266-3460

Northeast Headquarters
31 Tech Valley Drive
East Greenbush, NY 12061
+1 518-266-3460

MS-ISAC
MULTI-STATE
Information Sharing
& Analysis Center™

CYBER INCIDENT CHECKLIST

Center for
Internet Security®