OHIO AUDITOR OF STATE
KEITH FABER

OHIO AUDITOR OF STATE CYBERSECURITY CHECKLIST

PREPAREDNESS: WHAT TO DO

✓ Create a response plan and team
✓ Plan should include the office holder or head of the organization, IT, Legal, Finance and Public Relations at a minimum
✓ Establish clear action items
✓ Identify key contacts
✓ Know your reporting guidelines
✓ Encrypt sensitive data
✓ Map locations of critical data
✓ Restrict access
✓ Follow a retention policy
✓ Purge old employee accounts

REACTION: WHAT NOT TO DO

✓ Do NOT pretend it isn't happening
✓ Do NOT try to fix or look at computers and networks
✓ Do NOT turn off computers*
✓ Do NOT attempt to image computers
✓ Do NOT connect USB/storage devices or any other machine
✓ Do NOT run Antivirus or malware software
✓ Do NOT turn back on a machine or network if turned off

REACTION: WHAT TO DO

✓ Stop additional loss and contact IT immediately
✓ Have IT change security access and passwords if possible
✓ Respond to an arranged meeting area with plan
✓ Use your established reporting channel "privileged personnel only"
✓ Contact proper law enforcement
✓ Take note of date/time, persons involved etc. for notification and reporting requirements
✓ Wait for law enforcement/forensic experts to arrive
✓ Handle media requests

* - Unless you have a recent backup and/or are an IT professional. Shutting down your computer can disrupt the malware connection and potentially cause complete loss.