

PRE-INCIDENT CHECKLIST

Listed below are items you must have or do before you respond to a cybersecurity incident:

Have (and drill) a customized incident response plan

Identify who should be on your response team and what their responsibilities are

Gauge whether you currently have sufficient IT resources to respond to an incident or whether third-party support would be required

Document and practice lockdown procedures (for both your clients and your own systems)

Have cybersecurity insurance and/or lawyer(s)

Ensure that you have a clean system ready to restore, perhaps involving a complete reimage of a system or a full restore from a clean backup

Audit backups and practice backup restoration

Know how to retrieve/request access to relevant event and activity logs
Prepare a communication strategy and lawyer-approved scripts/templates for quick use

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

