

First Hour of a Cyber Incident

Practical tools from Acervus, free to use and share.

1. Isolate, do not erase. Disconnect affected systems from the network. Do not power them off, wipe, or reimage them; that destroys evidence.
2. Do not contact or pay the attacker.
3. Switch to out-of-band communication. Assume email and chat may be monitored; use phones or a separate account.
4. Write down what you know. Time of discovery, who found it, which systems, and what was observed. Take photos or screenshots.
5. Preserve logs. Do not delete files, logs, or accounts, even suspicious ones.
6. Hold off on sweeping changes. Mass password resets or system rebuilds can alert the attacker before their access is mapped. Make them on your responders' advice.
7. Notify the right people. Leadership, legal counsel, and your cyber insurer. Many policies require prompt notice and the use of approved response firms.
8. Consider reporting. In the United States, incidents can be reported to the FBI and to CISA.
9. Call for help. Report an Active Incident to Acervus through the urgent incident form on the Acervus website.