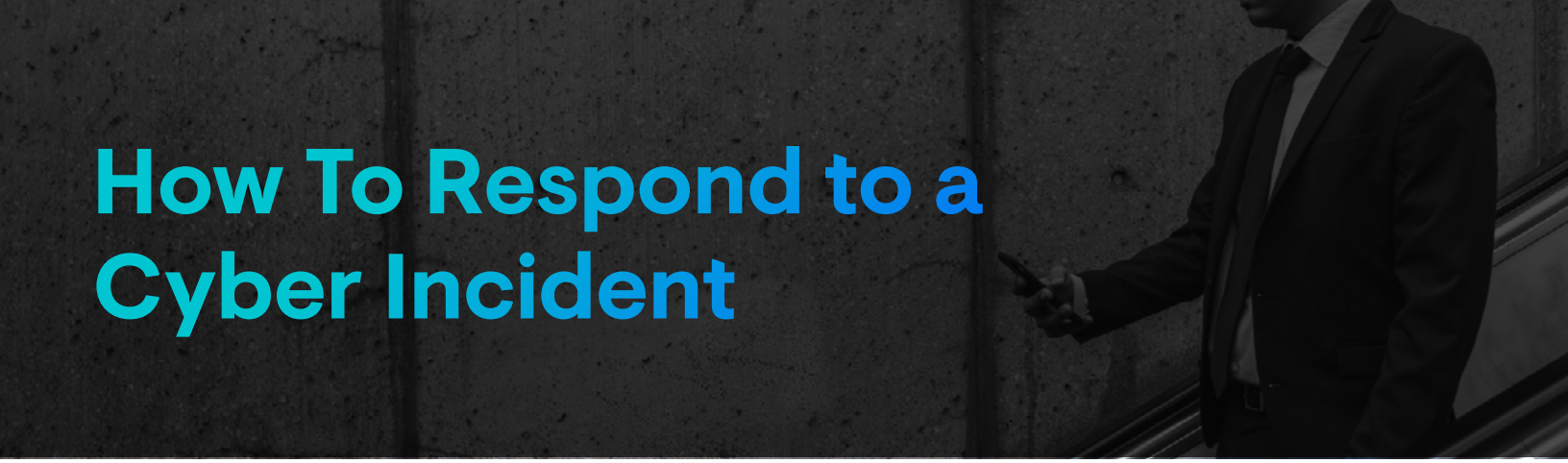

How To Respond to a Cyber Incident

CORE RULES

Listed below are items you must have or do before you respond to a cyber incident.

- ☐ Have an incident response (IR) plan.
- ☐ Test, maintain and communicate your IR plan.
- ☐ Train your team to the plan at least quarterly.
- ☐ Update the plan with learnings and changes quarterly.
- ☐ Communicate any and all changes to the plan.
- ☐ Ensure the right people are in the right IR roles (and have backups for key roles).
- ☐ Establish a relationship with a breach attorney.
- ☐ Understand attorney/client privilege.
- ☐ Understand insurance policies and coverages.
- ☐ Maintain copies of client's insurance policies.
- ☐ Make IR planning and testing a requirement with executive buy-in.
- ☐ Keep information about the cyber event to only those who need to know.
- ☐ Don't put anything in writing unless a breach attorney instructs you to do so.
- ☐ Don't use words like breach, hack or attack prematurely. Instead, consider using the word "incident."
- ☐ Do not sacrifice forensics data in favor of restoration.
- ☐ Rely on experts to help you, and establish these relationships with experts now—don't just wait until an event!

INCIDENT RESPONSE CHECKLIST

Use this checklist to help respond to a cyber incident in a swift and organized manner.

EXECUTIVE/BUSINESS PERSPECTIVE
Responsible for critical decision making and communications.

GET ON THE PHONE

- ☐ Contact your cybersecurity insurance carrier first. They will provide you with incident response and legal resources.
- ☐ Wait for your breach attorney to ensure you have attorney/client privilege.

ORGANIZE THE TROOPS

- ☐ Have your plan ready and your IR team in place. Make any adjustments if people are not available.
- ☐ Monitor your people and make sure they get food and rest. These events can introduce stressful elements that people have never faced. Consider working with a coach or mental health expert who can focus on maintaining team wellness and doing regular check-ins with everyone.
- ☐ Do not communicate with a threat actor. Leave that to your third-party IR and Legal experts.
- ☐ Listen to your experts.

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 emails.
- ☐ Run damage control with key affected clients.

ASSESS DAMAGE

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

GET YOUR STORY STRAIGHT

- ☐ Determine how much to share and with whom. Knowing what *not* to say is just as important as what you can say.
- ☐ Coordinate with team re: communication scripts/templates for both notifying and updating clients and responding to press inquiries.
- ☐ Ensure your messaging is approved by breach counsel. You need to ensure your internal (employee) messaging is treated with the same care and importance as external messaging.

TECHNICAL PERSPECTIVE
Responsible for containment, isolation and restoration.

LOCK DOWN AFFECTED CLIENTS

- ☐ Isolate affected client endpoints by taking them off the network.
- ☐ Do NOT power down or reboot any affected servers or endpoints. Disconnect them from the network to ensure memory forensics artifacts are preserved.
- ☐ Ensure backups are isolated/protected.

LOCK DOWN YOUR ACCOUNTS AND TOOLS

- ☐ Audit for unusual tasks, scripts, policy changes, etc.
- ☐ Disable user accounts associated with abnormal/malicious behavior and terminate those active sessions.
- ☐ Isolate any endpoints and other accounts associated with those users.
- ☐ Minimize logging into affected systems using privileged credentials.
- ☐ Ensure multi-factor authentication (MFA) is enabled on all accounts
- ☐ Confirm that antivirus (AV) or endpoint detection and response (EDR) tool is enabled and updated, then run a deep scan.
- ☐ Back up log files.

CONDUCT A REMEDIATION EVENT

- ☐ Once the incident has been properly scoped, a coordinated "remediation event" will increase the chances of successfully removing the threat actor from the environment.
- ☐ Cut off access to the environment.
- ☐ Reset passwords for all (or affected) accounts.
- ☐ Identify and patch the vulnerable systems.
- ☐ Remediate malware and/or malicious remote access tooling from systems.
- ☐ Reimage or remove systems as needed.
- ☐ Revert to clean backups from before the earliest known initial threat actor access.
- ☐ Monitor closely for any indications of re-infection.

COMPLETE A POST-EVENT ANALYSIS

- ☐ Ensure your team has the opportunity to candidly reflect on the event—the good, the bad and the ugly.
- ☐ Review how each person performed in their role. Determine if changes need to be made.
- ☐ Modify your IR plan, if required, to reflect the lesson learned.
- ☐ Schedule an IR tabletop test for your revised plan.