CYBERSECURITY INCIDENT RESPONSE CHECKLIST

Steps to take following the detection of a cyber incident

While forward-thinking business leaders know the risks and realities surrounding a data breach – and are implementing protective measures accordingly – no one is immune to attack. When your company believes a cyber incident has occurred, use the steps outlined here to contain the incident and minimize losses. (Note the specific actions – including the order of these steps – will vary on a case-by-case basis.)

We're here to help...

No two cyber incidents are the same, and neither are the response plans. After your company experiences a cyber incident, **get** the support of a Performance Improvement Partners cybersecurity expert. You'll find out the severity of the attack and understand steps you need to take to minimize threats.

And **remember**: Prevention is vastly cheaper than remediation following a breach.

Learn how to protect your business from cyber threats with a complimentary cybersecurity workshop, only available to Private Equity firms and their portfolio companies

Action	Completed
Detection and Analysis	
1. Confirm that an incident has occurred.	☐
▪ Analyze the precursors and indicators.	☐
▪ Look for correlating information. (E.g., check multiple indicator sources to validate the incident.)	☐
▪ Perform research. (E.g., check your knowledge base for error codes, use search engines to gain information on unusual activity, seek information and assistance from others.)	☐
▪ As soon as the IT/cybersecurity team believes an incident has occurred, begin documenting the investigation and gathering evidence.	☐
2. Prioritize handling the incident based on the relevant factors, including functional impact, information impact, and recoverability effort.	☐
3. Report the incident to the appropriate internal personnel and external organizations. At times this may include insurance providers and legal counsel – check with a cyber expert.	☐
Containment, Eradication, and Recovery	
4. Acquire, preserve, secure, and document evidence.	☐
5. Contain the incident: Based on the containment criteria (e.g. loss of data, evidence preservation), select and implement a containment strategy. (E.g., disconnect affected assets from the network, monitor activity to gain insight.)	☐
6. Eradicate the incident.	☐
▪ Identify and mitigate all vulnerabilities that were exploited.	☐
▪ Remove malware, inappropriate materials, and other components.	☐
▪ If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them.	☐
7. Recover from the incident.	☐
▪ Return affected systems to an operationally ready state.	☐
▪ Confirm that the affected systems are functioning normally.	☐
▪ If necessary, implement additional monitoring to look for future related activity.	☐
Post-incident Activity	
8. Create a follow-up report.	☐
9. Hold a retrospective to discuss learnings -- a mandatory step for major incidents, otherwise this is optional.	☐

If you're the victim of a cyber incident, contact PIP for immediate support.


203-220-9556


performance@pip-llc.com


pip-llc.com