Acronis

Incident response plan checklist

Validating or creating a cybersecurity IRP

Introduction

Below are items to consider before creating or updating an incident response plan. Check off any areas where you believe you have a proper process in place. Consider creating new processes for each of the remaining items, though not every process will be applicable to every business. The resulting list should help you craft a more complete incident response plan.

→ Total 27 questions

Preparation

Question	Current status	Improvement plan
Do you have current security policies and is everyone in the company aware of them?	Text up to 300 characters.	Text up to 300 characters.
Is your company ready to tackle cybersecurity incidents?	Text up to 300 characters.	Text up to 300 characters.
Do you have the ability to document and maintain the records of who discovered / reported the incident? Do you have the ability to document this securely?	Text up to 300 characters.	Text up to 300 characters.

Preparation

Question	Current status	Improvement plan
Have you already documented who is responsible for each phase of the incident response process?	Text up to 300 characters.	Text up to 300 characters.
Does the incident response team have the necessary tools to handle incidents?	Text up to 300 characters.	Text up to 300 characters.
Do you currently have documents/processes to follow depending on the type of incident?	Text up to 300 characters.	Text up to 300 characters.

Preparation

Question	Current status	Improvement plan
Do you have the ability to document and securely maintain records of incidents, including the time, location, business operations impact and IT infrastructure impact of every incident?	Text up to 300 characters.	Text up to 300 characters.
Have you documented who can interview personnel (internal and external) in the wake of an incident?	Text up to 300 characters.	Text up to 300 characters.

Containment

Question	Current status	Improvement plan
Can the incident be isolated? If yes, what were the steps taken and could you document them? If no, why could you not isolate the incident and document it?	Text up to 300 characters.	Text up to 300 characters.
Do you know if affected systems remain isolated from non-infected ones?	Text up to 300 characters.	Text up to 300 characters.
Are any backups available? Do you trust their integrity? Are they fully patched and cleaned of malware?	Text up to 300 characters.	Text up to 300 characters.

Containment

Question	Current status	Improvement plan
Do you have a process for making a copy of an infected system for forensics analysis?	Text up to 300 characters.	Text up to 300 characters.
Are you sure that the threat has been removed from infected systems?	Text up to 300 characters.	Text up to 300 characters.

Eradication

Question	Current status	Improvement plan
Have infected systems been patched for known vulnerabilities?	Text up to 300 characters.	Text up to 300 characters.
Do any systems or applications need to be reconfigured?	Text up to 300 characters.	Text up to 300 characters.
Have entry points been reviewed and closed if possible?	Text up to 300 characters.	Text up to 300 characters.

Eradication

Question	Current status	Improvement plan
Are any other defenses needed in order to eliminate the issue?	Text up to 300 characters.	Text up to 300 characters.
Are you sure the malicious activity has been removed from affected devices/workloads? Are you sure the threat actor has no more access?	Text up to 300 characters.	Text up to 300 characters.

Recovery

Question	Current status	Improvement plan
Have you documented the sources that incident responders are to use for recovery and backups?	Text up to 300 characters.	Text up to 300 characters.
Have you documented how the responders will safely restore infected workloads back into production?	Text up to 300 characters.	Text up to 300 characters.
How and when do you define when infected systems can be used?	Text up to 300 characters.	Text up to 300 characters.

Recovery

Question	Current status	Improvement plan
During a recovery, do you have documents related to what operations will be restored?	Text up to 300 characters.	Text up to 300 characters.
Do responders have the ability to document the entire recovery process?	Text up to 300 characters.	Text up to 300 characters.
Do you have a standard procedure to evaluate damages and costs from an incident (including the cost of damage as well as containment and recovery efforts)?	Text up to 300 characters.	Text up to 300 characters.

Recovery

Question	Current status	Improvement plan
Do you have a documented process for modifying policies, standard operating procedures and guidelines?	Text up to 300 characters.	Text up to 300 characters.
Do you have a documented process for conducting “lessons learned” post-mortem incident analysis? Do you have a list of questions to be answered in the document?	Text up to 300 characters.	Text up to 300 characters.
Do you store the documentation of your incident response processes in a secure place? Are your documents, e.g., contact lists, stored in a location and manner that makes them accessible during an incident, i.e., still available if a cyberattack brings the local network down?	Text up to 300 characters.	Text up to 300 characters.

Acronis

About Acronis Cyber Protect

Acronis is committed to helping businesses of all sizes manage cyber protection in a constantly evolving threat landscape. Acronis Cyber Protect delivers easy, efficient and secure cyber protection to help IT teams protect data from any threat. Available as a single solution featuring integrated backup and recovery, cybersecurity and endpoint protection, Acronis Cyber Protect gives IT teams 360-degree cyber protection for all their data and applications — whether a part of on-premises or remote systems, in private or public clouds or on desktop or mobile devices. To learn more, visit acronis.com today.