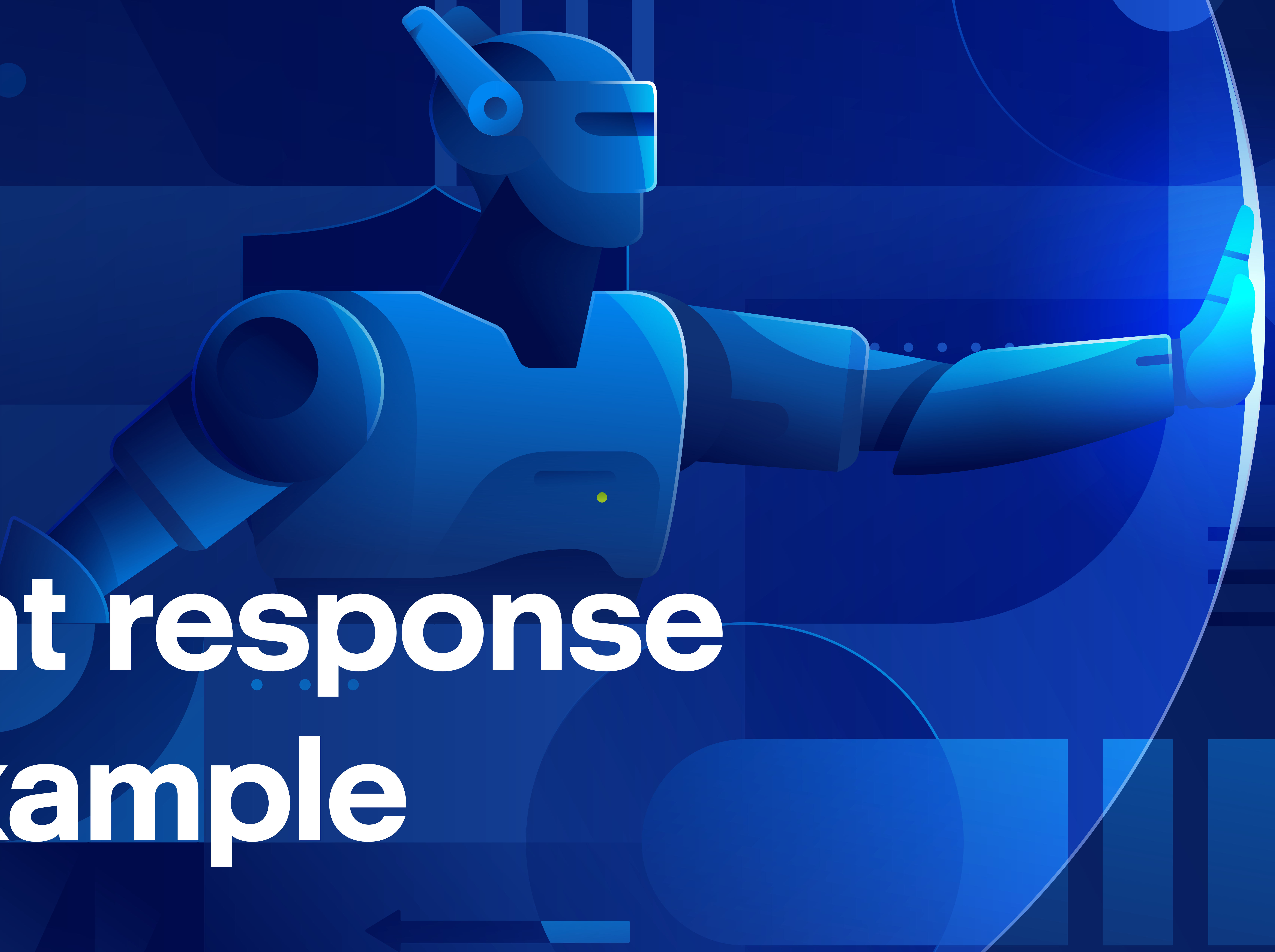
Acronis

Incident response plan example



Introduction

This document provides a best-practices example of the basic steps to take during an incident response. To create the plan, modify the steps in this example with your own contact information and specific courses of action for your organization.

Step 1

The person discovering the incident should first call the field / local office. The known sources should be provided with procedures to follow and a contact list. This list should include possible individuals and groups that might discover an incident. Sources that may require contact information include:

a. IT helpdesk
b. Physical security, e.g., personnel or third-party services monitoring for facilities break ins
c. System administrator
d. Firewall administrator
e. Business partners
f. Manager
g. Security department or a security person
h. Outside sources such as telecom service providers and other critical infrastructure contacts (utilities, public safety, etc.)

List all sources and verify contact details and procedures. Normally, each source would contact a 24/7 entity such as a grounds security office. Those in the IT department may have different contact procedures from those outside of IT.

Step 2

If the individual who detected the incident is an IT department member or the affected department, proceed to → Step 5

Step 3

If the individual who discovered the incident is not part of the IT department or the affected department, they should contact the security department, which can be reached 24 hours a day at (xxx) xxx-xxxx.

Step 4

The security office will refer the incident discoverer either to the IT emergency contact list or the affected department's contact list, directing them to call the designated numbers listed (in the order on the list). The security office will log:

a Caller's name

b Time of call

c Caller's contact information

d Incident type

e Equipment or persons involved

f Location of equipment or persons involved

g How the incident was discovered / detected

h Time of day the incident was first noticed that supports the idea that an incident occurred

Step 5

The IT employee or affected department employee who receives (or has discovered) the incident will refer to their contact list of managers and members of the incident response team. The employee calls the personnel named on this list and then contacts the incident response manager by both email and telephone, while ensuring other suitable backup employees and designated managers are contacted. The employee logs the received information in a format similar to the security office's in the preceding step. The employee might add:

a. Whether the affected device is business critical
b. Severity of the potential impact
c. Name of the target system, its operating system and revision level, IP address and physical location
d. Any other information about the source of the attack

Step 6

Members of the response team who have been contacted will meet to discuss the situation (via phone session) and then set out and craft a response strategy, including:

a. Is the incident genuine or a false alarm?
b. Is the incident still in progress?
c. What data and / or physical property is under threat, and how critical are these resources?
d. What would be the impact on the business if the attack / incident should continue unimpeded: minimal, serious or critical?

e. What systems have been affected or are the target? Where are they located physically and in the network?
f. Does the incident fall inside the trusted network?
g. Is the response urgent?
h. Can the incident be contained quickly?
i. Will the response alert the attacker (and do we care if it does)?
j. What type of incident is it? Examples include virus, worm, intrusion, abuse and damage

Step 7

The response team creates an incident ticket and assigns it a severity level as follows:

a. Category one — A threat to life or public safety
b. Category two — A threat to sensitive data
c. Category three — A threat to computer systems
d. Category four — An interruption of services

Step 8

The response team assesses the incident to determine which procedure defines the appropriate response:

a. Worm response procedure
b. Virus response procedure
c. System failure procedure

d. Active intrusion response procedure — Is critical data at risk?
e. Inactive intrusion response procedure
f. System abuse procedure
g. Property theft response procedure
h. Denial of service procedure
i. Database or file denial-of-service response procedure
j. Spyware response procedure

The team should also develop procedures in addition to the examples provided in this document. In the absence of an applicable procedure, the team must document the actions taken and later create a procedure to follow in the event of similar incidents.

Step 9

The team members will employ forensic techniques, including reviewing system logs and any forensic backups, looking for gaps and loopholes in logs, reviewing intrusion detection logs, and questioning witnesses and victims of the incident to determine the cause(s). Only authorized staff (which may vary depending on the incident type) should conduct interviews or review evidence.

Step 10 Members of the team will recommend modifications to prevent a repeat of the event or other systems from being infected.

Step 11 With the approval of management, these modifications would then be implemented.

Step 12 The team members will restore the affected systems to a clean state with one or more of the following measures:

a. Rebuild the affected system(s) from scratch and, if necessary, restore data from backups. Preserve evidence before doing so
b. Have users change passwords, if passwords may have been compromised
c. Ensure that affected systems have been hardened by disabling or removing unused services
d. Ensure that any known vulnerabilities in operating systems and applications have been completely patched
e. Ensure that antivirus protection and intrusion detection are running in real time
f. Ensure that system logs reflect actual events correctly and are set at the appropriate level of verboseness

Step 13 The team should promptly document the following:

a. How the incident was discovered
b. Category of incident severity

c. How the incident occurred (email, firewall, etc.)

d. Where the attack originated (such as IP addresses and other related information about the attacker)

e. Which response procedures were used

f. The actual steps performed from those procedures

g. Whether the response was effective

Step 14

The team will preserve all relevant evidence — making copies of logs, emails and other communications. The teams will keep witness lists and evidence as long as needed to complete prosecution (and beyond) in the event of an appeal.

Step 15

The team will notify appropriate external authorities, including local law enforcement, national law enforcement, and other appropriate authorities if it is possible to prosecute the intruder (list the agencies and contact numbers here).

Step 16

The team will evaluate and estimate damages to the organization, their direct costs, and the costs of containment and recovery efforts.

Step 17

The team will review the response and update the organization’s policies and procedures to include any new measures to prevent a recurrence of the incident:

a. Evaluate whether additional policies could have stopped the intrusion
b. Consider whether an unfollowed procedure or policy enabled the intrusion and then what might be changed to ensure the process or policy is followed in the future
c. Determine whether the response to the incident was appropriate and effective, and how it might be improved
d. Determine whether every suitable party was informed in a timely manner
e. Determine whether the procedures for responding to the incident were documented with adequate detail, if they effectively addressed the incident, and how they could be improved
f. Verify that all possible remediations have been taken to prevent reinfection (examples: patching of known vulnerabilities, system lockdowns, password changes, antivirus updates, application of appropriate email policies, etc.)
g. Consider what policy and procedural changes might be adopted to prevent new and similar infections
h. Determine whether any security policies need to be updated
j. Document all lessons learned from the incident and its response

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.