3 Must-Haves in Your Cybersecurity Incident Response

Planning End-to-End Incident Response — Before It's Needed

Gartner

Prepare to Act Fast During an Incident

Cybersecurity incidents are a matter of “when,” not “if.” They result in more adverse media coverage than ever before, and auditors, regulators and other stakeholders expect organizations to demonstrate a clear plan for managing these incidents to minimize the impact on brand, reputation, staff, customers and shareholders.

The imperative for security and risk management leaders is to prepare. The key tools are a documented response plan and a detailed playbook for the incident type.

This guide excerpts pages from Gartner tools and playbooks*. All detail is illustrative.

*Complete tools are available to certain Gartner clients: Toolkit: Cybersecurity Incident Response Plan, Toolkit: Creating a Ransomware Playbook and Toolkit: Tabletop Exercise for Cyberattack Preparation and Response. Clients can download the templates to customize and submit them for review by Gartner experts, who can also answer interim questions on your evolving plan.

2021 saw the highest average breach cost in 17 years, and **10% of breaches involved ransomware** — double the frequency seen in 2020.

Source: IBM Cost of a Data Breach Report, 2021; Verizon 2021 Data Breach Investigations Report

Three Components You Must Get Right

01

Build an incident response plan

A general plan for responding to cyberincidents

Data breach costs rose from $3.86 million in 2020, to **$4.24 million** in 2021.

Source: IBM Cost of a Data Breach Report, 2021

02

Develop detailed response playbooks

Detailed guides for handling specific incident scenarios

Over **80%** of ransomware attacks involve data theft in addition to encryption.

Source: Ransomware attackers downshift to "Mid-Game" hunting in Q3 2021, Coveware, October 2021

03

Conduct regular tabletop exercises

Routine tests to practice incident response plans

Ransomware attacks create an average **23 days** of downtime.

Source: Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority, Coveware, July 2021

Three Components You Must Get Right

01

Build an incident response plan

A general plan for responding to cyberincidents

02

Develop detailed response playbooks

Detailed guides for handling specific incident scenarios

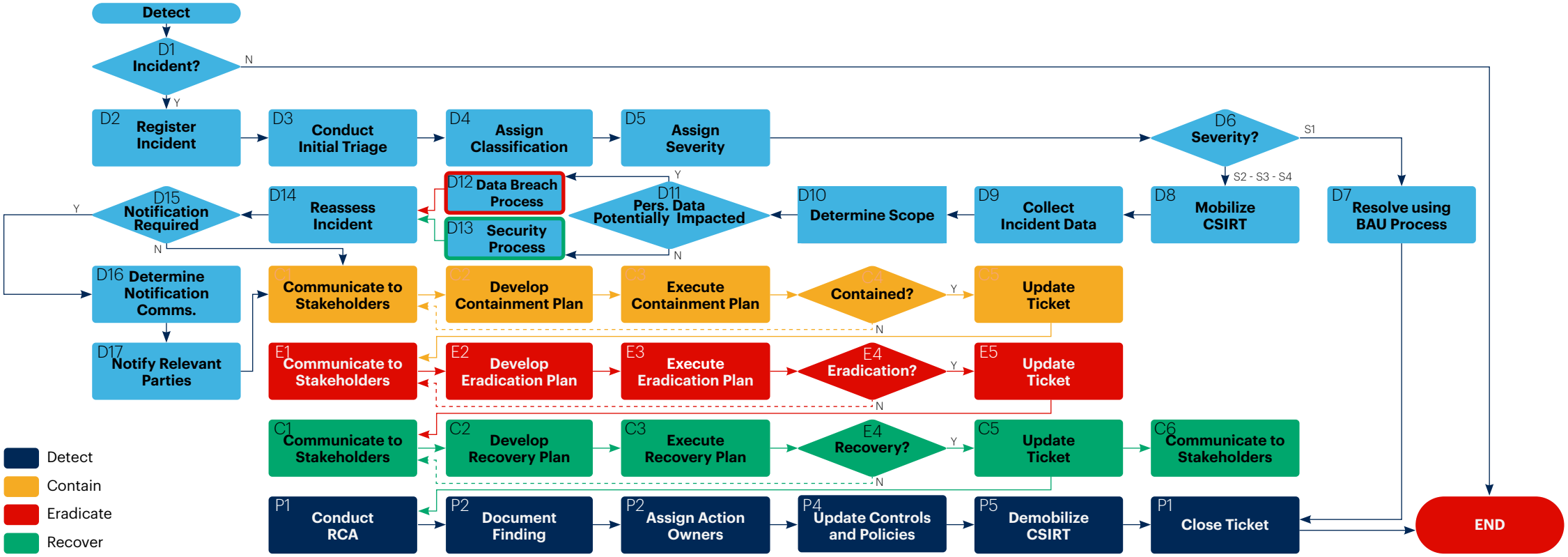
03

Conduct regular tabletop exercises

Routine tests to practice incident response plans

Develop a Response Process Map

The incident response plan should dictate detailed, sequential procedures to follow in the event of an incident. The incident coordinator (or similar role) should ensure that each step of the process is completed and that progress is tracked and communicated on a rolling basis.



Define Incident Severity Tiers

All security incidents must be triaged and assigned a severity tier. This helps to guide incident escalations, assign service-level agreements and otherwise inform stakeholders of the potential or realized impact of an incident on the organization. The severity also drives who is notified, what the escalation path will be and, therefore, which playbook to communicate.

Severity	Business Impact					Technical Attributes	
Tier	Safety	Legal	Regulatory	Financial	Reputational	Data Class	Operations
04 Cyber Crisis	Severe Injuries/Death	Significant Impact	Fines: $Z+	Loss: $Z+	Global Media	Top Secret	Catastrophic Outage
03 High	Serious Injuries	Moderate Impact	Fines: $Y – $Z	Loss: $Y – $Z	National Media	Secret	Major Outage
02 Medium	First Aid	Low Impact	Fines: $X – $Y	Loss: $X – $Y	Local Media	Internal	Minor Outage
01 Low	No Injuries	No Impact	No Violations	No Loss	No Harm	Public	No Outage

Assign Roles and Responsibilities

Effective incident response is a team sport. Maintain a RACI chart that indicates all of the roles and responsibilities for incident response across the organization. Common stakeholders to include are the C-suite, legal, privacy and HR teams.

Step	CIO	CISO	DPO	Help Desk	Incident Coordinator	IT	SOC	Data Owner	Legal	PR	HR	Customer Operations
Register incident				AR	CI	I						
Conduct initial triage		I			AR	C		I	I			
Assign classification		I	I		AR			C	C			
Assign severity		I	I		AR			C	C			
Determine next steps based on severity	I	CI	CI		AR	C						
Resolve using usual process				I	I	AR		CI				
Mobilize CSIR team	I	I		I	AR	CI						

Three Components You Must Get Right

01

Build an incident response plan

A general plan for responding to cyberincidents

02

Develop detailed response playbooks

Detailed guides for handling specific incident scenarios

03

Conduct regular tabletop exercises

Routine tests to practice incident response plans

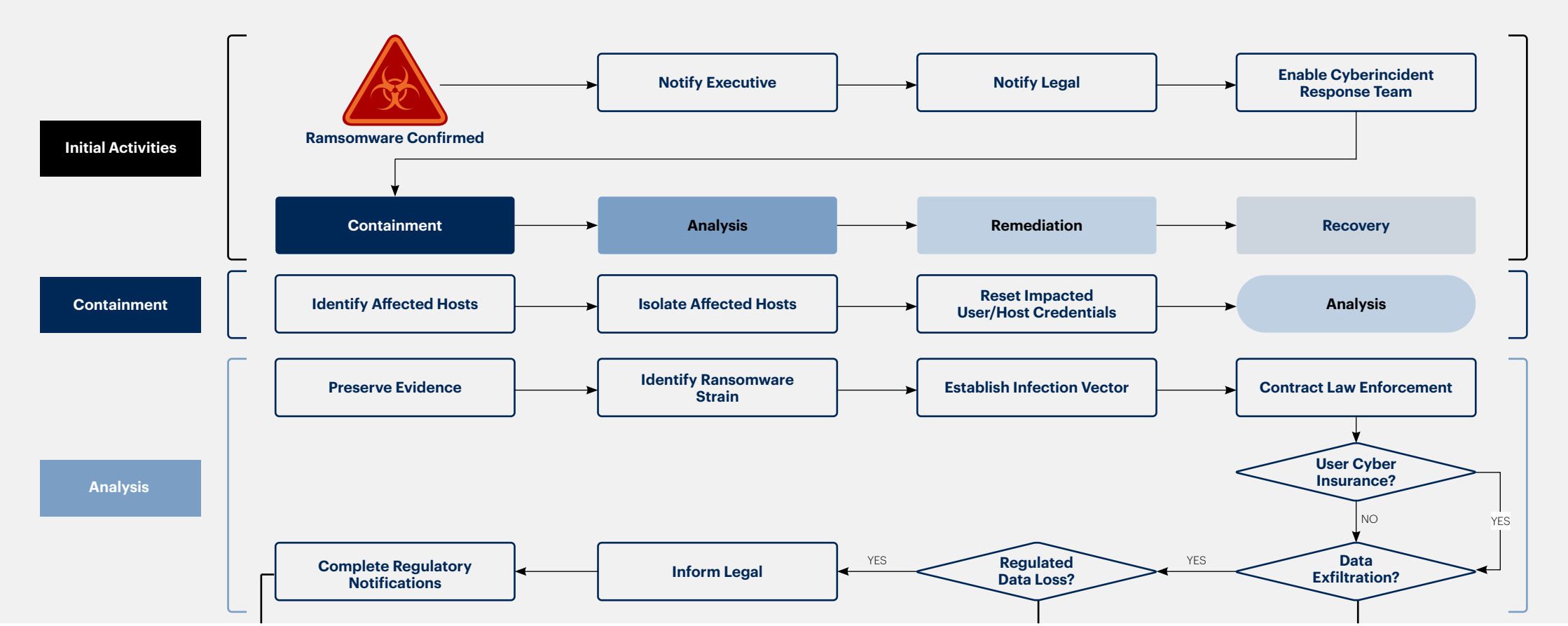
Create Response Playbooks

The CSIR team should develop specific playbooks for common or high-impact incident types — such as ransomware, as shown in this example. Response playbooks are designed to provide detailed guidance and procedures that go beyond security's general incident response plan.

Contents

Develop a Ransomware Response Process

Create a ransomware response process and decision tree. This process can then be used to develop detailed response procedures, assign roles and responsibilities and develop additional documentation the CSIR team can use to guide their response.



Document Detailed Response Procedures

Work with subject matter experts (SMEs) to document detailed ransomware response procedures. These procedures should include specific guidance, tools, example, settings, etc. — and should clearly identify responsible parties for every step.

	Process	Tasks	Responsible Party
CONTAINMENT	**Identify Affected Hosts**	1. Identify all hosts with reported ransomware 2. Conduct investigation to identify other potential infected devices. Potential indicators of compromise (IoC) could be: • **Anomalous file activity** – high volume of file renaming, high volume writes to local disks, disks enc • **Increased CPU and disk activity on endpoints** – self-explanatory • **Inability to access files** – self-explanatory • **Application failure** – self-explanatory • **Suspicious network traffic** – traffic across nonstandard ports, changes in typical packet sizes, changes in top hosts generating traffic, increase in "blocked" or "denied" entries in firewall logs • **Anomalies in privileged user account activity** – new account creation, changes to existing user/group permissions, change in ownership • **Geographical irregularities** – access from irregular geographies • **Suspicious registry or system file changes** – self-explanatory • **DNS request anomalies** – spike in traffic to previously unseen IPs	CSIRT CSIRT
	Do NOT power off machines without guidance from forensic investigators — doing so may destroy valuable forensic data residing in memory or executing on disk.		
	Isolate Affected Hosts	1. Disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based. 2. Consider whether turning off your Wi-Fi, disabling any core network connections (including switches), and disconnecting the entire network from the internet will be necessary.	CSIRT CSIRT

Three Components You Must Get Right

01

Build an incident response plan

A general plan for responding to cyberincidents

02

Develop detailed response playbooks

Detailed guides for handling specific incident scenarios

03

Conduct regular tabletop exercises

Routine tests to practice incident response plans

Create an Agenda and Invite Participants

Incident response tabletop exercises should include leadership and decision makers across the organization. A successful tabletop defines specific objectives and is highly structured to cover preplanned scenarios to which participants must react.

Agenda and Schedule — 90-Minute Tabletop Exercise

01	**Welcome and Introductions**	<5-minute time span>
02	**Exercise Objectives and Rules of Engagement**	<5-minute time span>
03	**Exercise Setup**	<5-minute time span>
04	**Scenario-Driven Exercise**	<60-minute time span>
05	**Group Debrief/Lessons Learned**	<15-minute time span>

Develop an Incident Scenario and Scenes

Cybersecurity tabletop exercises are most effective when structured as an initial scenario (e.g., malware), followed by a series of scenes that add new information to the incident to which participants must react. This structure replicates the uncertainty and evolution of real incidents.

	Elapsed Time Frame: Five Hours	Actual Time Frame: 60 Minutes
Scene No. 0: Initial Scenario	8:00 a.m.	10 Minutes
Scene No. 1: T + 30 Minutes	8:30 a.m.	10 Minutes
Scene No. 2: T + 1 Hour	9:00 a.m.	15 Minutes
Scene No. 3: T + 3 Hours	11:00 a.m.	5 Minutes
Scene No. 4: T + 4 Hours	12:00 p.m.	8 Minutes
Scene No. 4: T + 4.5 Hours	12:30 p.m.	7 Minutes

Craft Challenging Incident Scenes

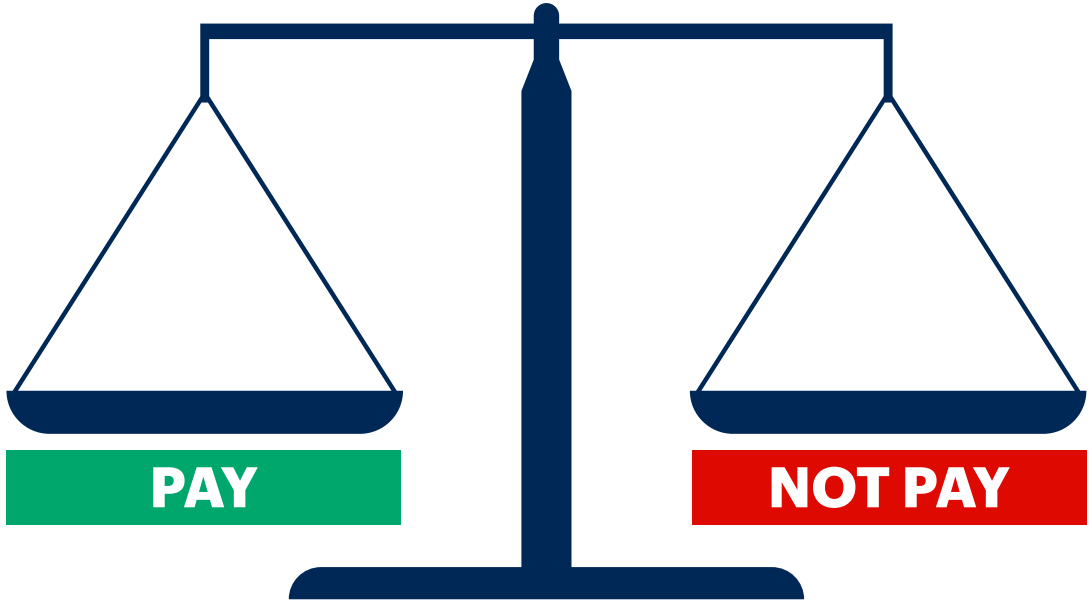
Tabletop exercises should replicate challenging questions that stakeholders must address during an actual attack.

Example: Ransomware
In a tabletop exercise, you can challenge participants to react to a ransom demand from an attacker.

Things to consider

The realities around paying a ransom include:

- On average, only 65% of the data is recovered, and only 8% of organizations manage to recover all data.
- Encrypted files are often unrecoverable.
- Attacker-provided decrypters may crash or fail.
- Recovering data can take several weeks.
- There is no guarantee that the hackers will delete the stolen data. They could sell or disclose the information later if it has value.
- It may be easier and cheaper to pay the ransom than to recover from backup, but that only encourages criminal behavior.
- In some cases, paying the ransom could even be illegal.



Gartner Cybersecurity Team*

Director Analyst
Security & Risk Management

Cybersecurity expertise:

- Reviews cybersecurity incident response plans; offers guidance on security awareness, metrics and security.
- Advises CISOs and their teams in security and risk practices and communications.
- 10 years' experience as an analyst and researcher.

Based in U.S.

Paul Furtado
Senior Director Analyst
Security & Risk Management

Cybersecurity expertise:

- Provides insight and advice on cybersecurity strategy, risk and incident response.
- Midsize enterprise (MSE) security specialty.
- 25+ years' experience as a CIO and CISO.

Based in Canada.

Wam Voster
Senior Director Analyst
Security & Risk Management

Cybersecurity expertise:

- Advises on the security of operational technology (OT) as well as security management, organization and governance.
- 30+ years as an IT practitioner, directing and advising security programs in complex environments (oil and gas, and fast-moving consumer goods sectors).

Based in the Netherlands.

*Some Gartner subscriptions allow clients to submit their cybersecurity incident response plans for review by Gartner experts or pose interim questions on their evolving plans.

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

eBook

3 Steps to Stop Employees Taking Cyber Bait

Change employee behavior and manage risks effectively.

Download eBook

Roadmap

Protect Your Business Assets With a Roadmap for Maturing Information Security Program

Build a mature program to mitigate cybersecurity risk effectively.

Download Roadmap

Webinar

Identify and Embrace New Collar Workers to Boost Cybersecurity

Explore nontraditional education forums that provide sufficient training.

Watch Now

Research

How to Prepare for Ransomware Attacks

Be ready for the security challenges organizations are facing today.

Download Research

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Gartner®