3 Must-Haves in Your Cybersecurity Incident Response

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

Gartner

Introduction

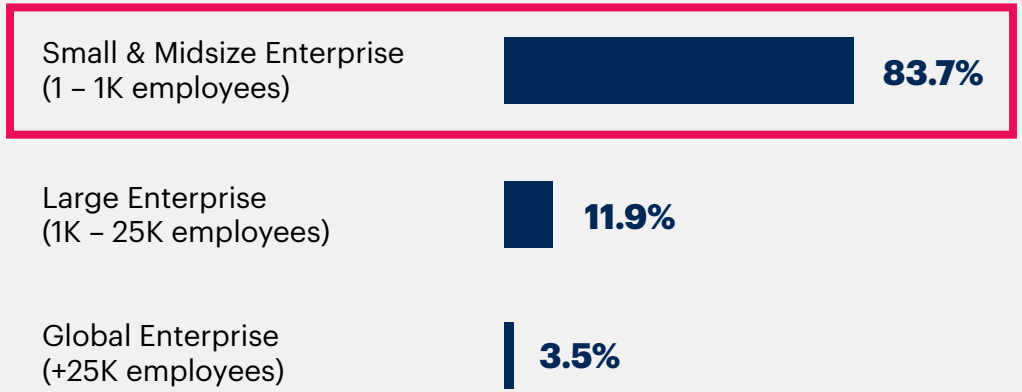
Small and midsize enterprises (MSEs) do not have the dedicated security teams or security tools of larger enterprises. As a result, they are the most targeted segment for ransomware attacks. Additionally, security efforts are typically distributed across a team focused on providing access and availability to the business, not security.

Defending against a security incident is not an easy task for organizations of any size. However, it is doable. Preparation is the best tactic an MSE can implement for combating any security incident. Creating and testing a comprehensive incident response plan will provide the tactical and technical guidance needed to mitigate the impact of a security incident and accelerate the recovery process.

The only thing harder than defending yourself against a cybersecurity incident is explaining to your board, CEO and customers why you weren't ready to address it quickly and effectively.

Paul Furtado
Senior Director Analyst

Ransomware by Victim Enterprise Size



Source: Coveware Ransomware 2021 Q3 Report

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.

Ransomware payments surpassed **US$ 1 billion** in 2023 — an all-time record high.

24% of cybersecurity incidents involved ransomware.

The Chainalysis 2024 Crypto Crime Report; Cost of data breach, IBM 2023

3 Components You Must Get Right

01

Build an incident response plan

A general plan for responding to cyberincidents

The average cost of a data breach reached an all-time high in 2023 of US$ **4.45 million.** This represents a 2.3% increase from the 2022 cost of US$ 4.35 million. Taking a long-term view, the average cost has increased 15.3% from US$ 3.86 million in the 2020 report.

Source: IBM Cost of a Data Breach Report, 2023

02

Develop detailed response playbooks

Detailed guides for handling specific incident scenarios

In 2023, **51%** of organizations worldwide did not have a ransomware incident response plan.

Source: 2023 Thales Data Threat Report

03

Conduct regular tabletop exercises

Routine tests to practice incident response plans

10% of organizations were hit by attempted ransomware attacks in 2023.

Source: Check Point Research: 2023 — The year of Mega Ransomware attacks with unprecedented impact on global organizations

3 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

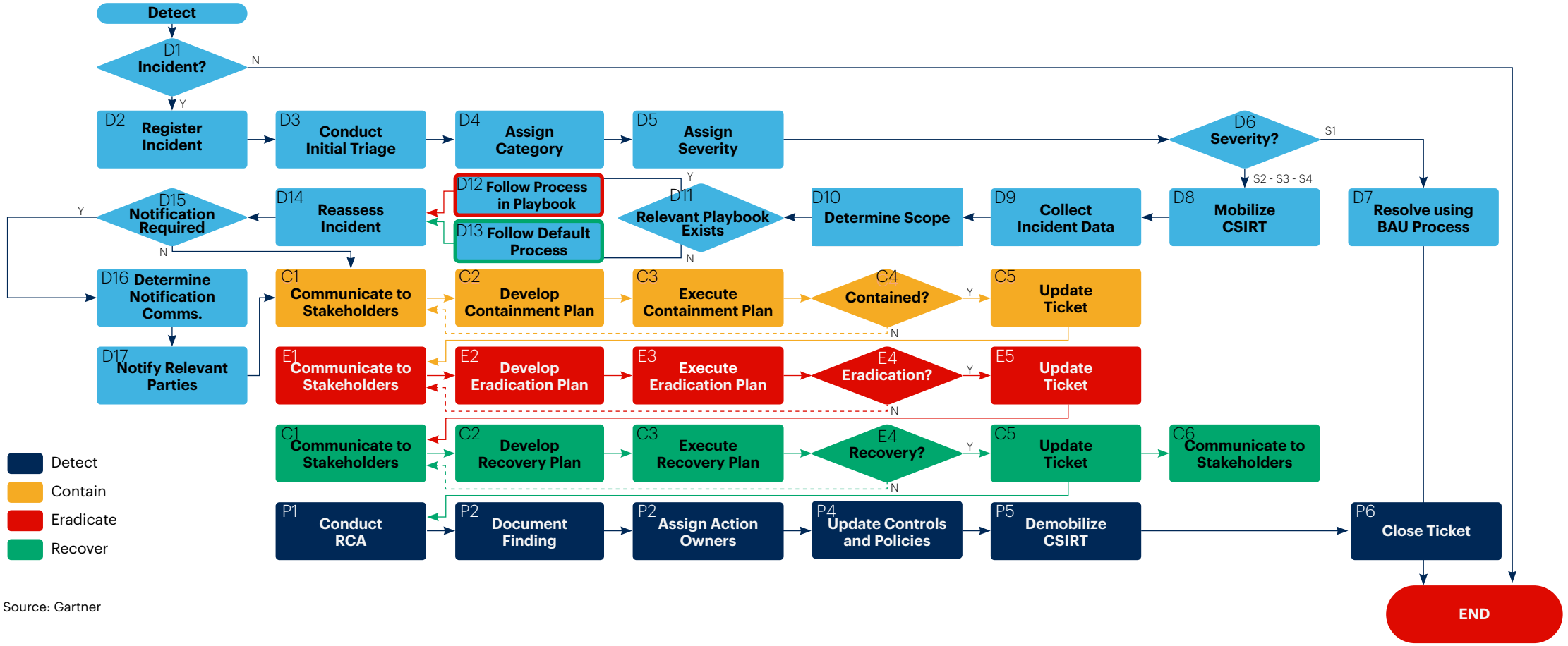
03

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.



Source: Gartner

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.

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

Source: Gartner

Define Escalation Paths

Effective incident response is a team sport. Maintain clear escalation paths based on the severity of the incident.

Severity	Escalation Path					
Tier	Note: Escalations are cumulative as the severity tier increases					
04 Cyber Crisis	CEO	CFO	Board	–	–	–
03 High	HR	Legal	COO	Privacy	PR	Cybersecurity Insurance
02 Medium	CISO	CIO	–	–	–	–
01 Low	Incident Handler	CSIRT	–	–	–	–

Source: Gartner

3 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.

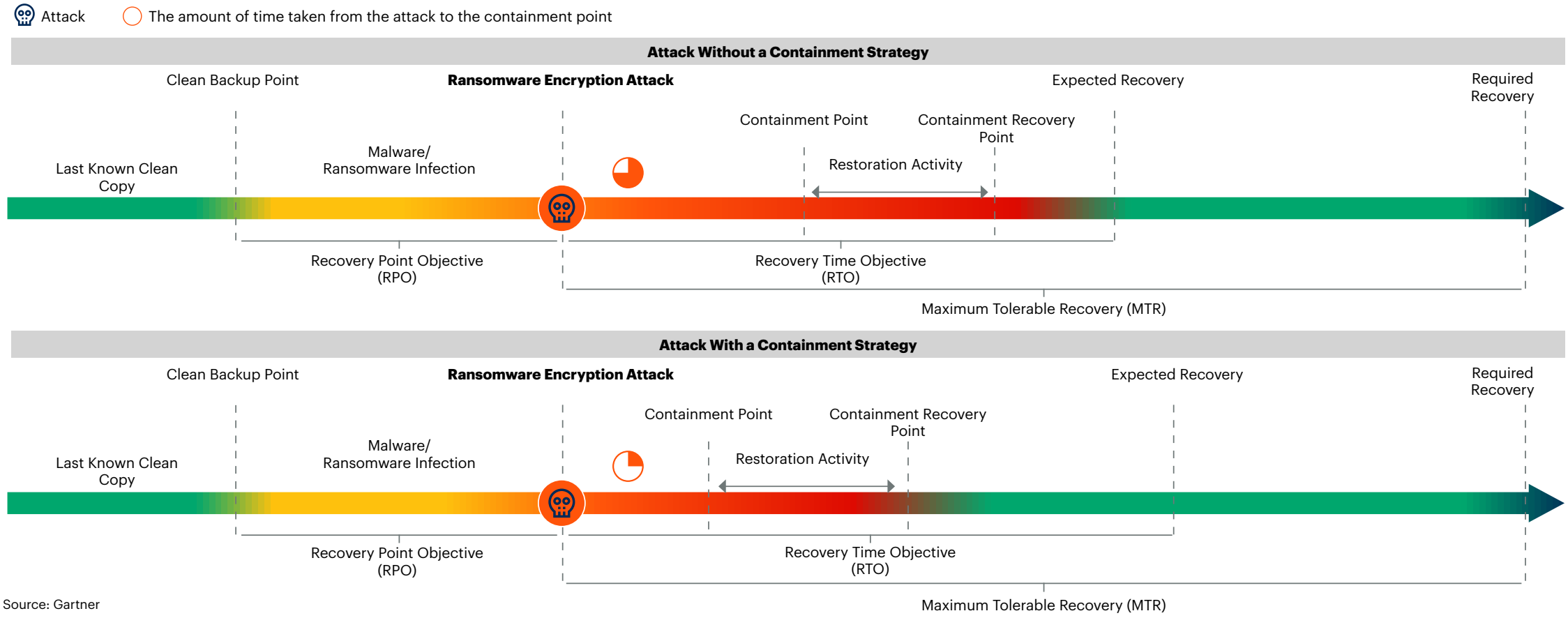
Contents

How to Use This Toolkit **1**
Prerequisites **1**
Minimum Requirements in IRP 1
Scope **1**
Initial Notification **2**
Four Phases of Ransomware Response **2**
Containment 2
Analysis 3
Remediation 3
Recovery 3
wFour Phases of Ransomware Response Workflow Diagram 4
Containment **5**
Identify Affected Hosts 5
Isolate Affected Hosts 5
Reset Impacted User/Host Credentials 5
Analysis **5**
Preserve Evidence 5
Identify Ransomware Strain 6
Establish Infection Vector 6

Source: Gartner

Develop a Containment Workflow

To help improve an organization's resilience during a ransomware attack, CISOs should work with stakeholders to develop a containment strategy. The key objective of this strategy is to reduce the time from the attack to the containment point while limiting the disruption within the business.



Source: Gartner

3 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>

Source: Gartner

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

Source: Gartner

Craft Challenging Incident Scenes

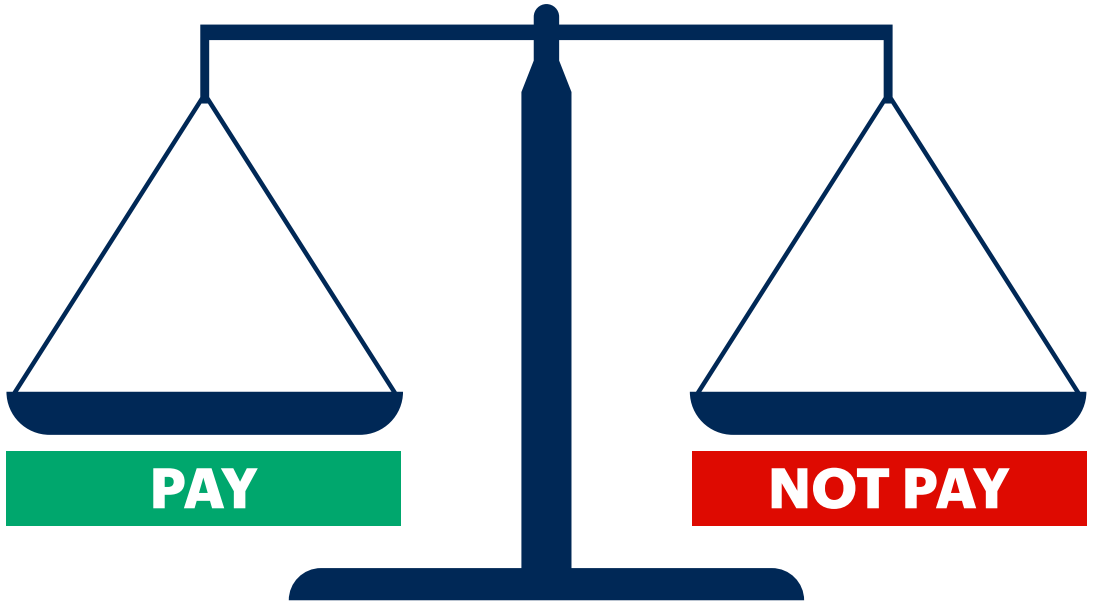
Tabletop exercises should replicate challenging questions that stakeholders must address during an actual attack.

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:

- Encrypted files are often unrecoverable.
- Attacker-provided decrypters may crash or fail.
- Recovering data can take significant time.
- 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.



Source: Gartner

Actionable, objective insight

Explore these additional complimentary resources and tools for security and risk leaders:

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

Product

How Gartner Works With CISOs

Find out how Gartner equips CISOs and their teams with the insight, guidance and tools.

Learn More

Webinar

The Gartner Emerging Technologies and Trends in Security for 2024

Explore the latest trends and their impact on security strategies and market dynamics.

Watch Now

eBook

4 Ways to Achieve Secure Employee Behaviors

Manage human risk and build a security-conscious organization.

Download eBook

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

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 3301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insights

Gartner®