3 Must-Haves in Your Cybersecurity Incident Response for Midsize Enterprises

Planning End-to-End Incident Response — Before it’s Needed
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

<table>
<thead>
<tr>
<th>Ransomware by Victim Enterprise Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small &amp; Midsize Enterprise (1 – 1K employees)</td>
</tr>
<tr>
<td>Large Enterprise (1K – 25K employees)</td>
</tr>
<tr>
<td>Global Enterprise (+25K employees)</td>
</tr>
</tbody>
</table>

Source: Coverware 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.

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

*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.

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

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

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

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.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Safety</th>
<th>Legal</th>
<th>Regulatory</th>
<th>Financial</th>
<th>Reputational</th>
<th>Data Class</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Crisis</td>
<td>Severe Injuries/Death</td>
<td>Significant Impact</td>
<td>Fines: $Z+</td>
<td>Loss: $Z+</td>
<td>Global Media</td>
<td>Top Secret</td>
<td>Catastrophic Outage</td>
</tr>
<tr>
<td>Medium</td>
<td>First Aid</td>
<td>Low Impact</td>
<td>Fines: $X – $Y</td>
<td>Loss: $X – $Y</td>
<td>Local Media</td>
<td>Internal</td>
<td>Minor Outage</td>
</tr>
<tr>
<td>Low</td>
<td>No Injuries</td>
<td>No Impact</td>
<td>No Violations</td>
<td>No Loss</td>
<td>No Harm</td>
<td>Public</td>
<td>No Outage</td>
</tr>
</tbody>
</table>
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.

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

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

**Develop a Ransomware Response Process**

Excerpt from Gartner Toolkit: Creating a Ransomware Playbook

1. **Initial Activities**
   - Identify Affected Hosts
   - Isolate Affected Hosts
   - Preserve Evidence
   - Identify Ransomware Strain
   - Establish Infection Vector

2. **Containment**
   - Notify Executive
   - Notify Legal
   - Enable Cyberincident Response Team

3. **Analysis**
   - Reset Impacted User/Host Credentials
   - Contract Law Enforcement

4. **Remediation**
   - Recover

5. **Complete Regulatory Notifications**
   - Regulated Data Loss?
   - Data Exfiltration?

**Questions:****

- User Cyber Insurance?
- Data Exfiltration?
# 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.

## Containment

<table>
<thead>
<tr>
<th>Process</th>
<th>Tasks</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Affected Hosts</td>
<td>1. Identify all hosts with reported ransomware</td>
<td>CSIRT</td>
</tr>
<tr>
<td></td>
<td>2. Conduct investigation to identify other potential infected devices.</td>
<td>CSIRT</td>
</tr>
<tr>
<td></td>
<td>Potential indicators of compromise (IoC) could be:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Anomalous file activity – high volume of file renaming, high volume writes to local disks, disks enc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Increased CPU and disk activity on endpoints – self-explanatory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inability to access files – self-explanatory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Application failure – self-explanatory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Suspicious network traffic – traffic across non-standard ports, changes in typical packet sizes, changes in top hosts generating traffic, increase in “blocked” or “denied” entries in firewall logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Anomalies in privileged user account activity – new account creation, changes to existing user/group permissions, change in ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Geographical irregularities – access from irregular geographies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Suspicious registry or system file changes – self-explanatory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DNS request anomalies – spike in traffic to previously unseen IPs</td>
<td></td>
</tr>
</tbody>
</table>

**Do NOT power off machines without guidance from forensic investigators — doing so may destroy valuable forensic data residing in memory or executing on disk.**

<table>
<thead>
<tr>
<th>Isolate Affected Hosts</th>
<th>1. Disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.</th>
<th>CSIRT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
<td>CSIRT</td>
</tr>
</tbody>
</table>
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**

| 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 |

**Actual Time Frame: 60 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.
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.

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.

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.

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

- **ebook**
  - Emerging Technology Roadmap for Midsize Enterprises
  - Benchmark your plans and make confident investment decisions.
  - Download eBook

- **ebook**
  - Top Strategic Technology Trends for 2022
  - Explore the 12 trends shaping the future of digital business.
  - Explore Trends

- **Roadmap**
  - The IT Roadmap for Digital Business Transformation
  - Avoid pitfalls and lead smart, effective digital transformations.
  - Get Roadmap

- **Webinar**
  - API-First Strategy for Midsize Enterprise Business Model Transformation
  - Discover how you can enable business model transformation.
  - Watch Now

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

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

Stay connected to the latest insights  

© 2022 Gartner, Inc. All rights reserved. CM_GTS_1654714