Mandiant

White paper

Best practices for incident response planning

A cyberattack can severely disrupt business operations if your organization hasn’t created an incident response plan. Here’s what you need to know.

"Most organizations have done an admirable job equipping themselves with sophisticated cybersecurity tools, leading to strong capabilities in detection and response," says Ryan Fried, principal security consultant with Mandiant. "However, they often lack a tested, actionable incident response plan (IRP), and without one, attackers can linger deep inside the environment when rapid action is paramount."

Mandiant's frontline responders continue to see the same scenarios — such as unclear roles, slow decision-making, and communication failures — that can escalate a manageable threat into a full-blown crisis. Mandiant consultants are regularly on the front lines of cyber incidents, where they conduct in-depth investigations and analysis of the most recent attacks. This firsthand experience results in a deep understanding of threats and the effective strategies required to defend against them.

Despite mounting risks, many enterprises don't have a usable IRP. They may have a document in place, but it's outdated, untested, or so long and broad that it fails to support real-world response in a crisis or recovery. Without proper preparation, organizations can't move quickly when it matters most.

This short guide draws on insights from Mandiant's 20+ years of breach response and the latest threat intelligence to explain:

- Why IRPs are essential
- What these plans must include
- How Mandiant's incident readiness services, including the Mandiant Retainer, help organizations respond with confidence

Incident response planning is both a technical and executive-level business imperative

In the face of modern cyber threats, an IRP is a business necessity. A well-defined plan minimizes disruption, ensures regulatory compliance, and helps leadership act with clarity during high-stakes situations.

The consequences of uncertainty are significant. Delays in response allow attackers more time to move laterally, encrypt systems, or exfiltrate data. Disjointed communications frustrate recovery efforts and damage trust with customers, regulators, and partners.

"Critical information such as contact details may be incorrect or outdated, and communication plans might be stale," Fried says. "Consequently, it is often unclear what criteria justifies invoking the incident response plan and who is authorized to do so."

An IRP helps address these challenges by identifying clearly defined roles, processes, and protocols — including alternates if roles or personnel change. It empowers stakeholders to act quickly and decisively, reducing confusion and ensuring alignment during a crisis.

Emerging threats underscore the need for preparedness

The threat landscape is shifting rapidly. M-Trends 2025 research found:

- Mandiant identified and began tracking 737 new threat clusters.
- The top initial infection vectors were exploits (33%), stolen credentials (16%), and phishing (14%).
- Median dwell time rose to 11 days in 2024, reversing the downward trend seen in prior years.

These trends demand new levels of preparation. “Ransomware, data theft extortion, and multifaceted extortion continue to be the most disruptive type of cybercrime globally due to both the volume of intrusions and potential scope of damage,” says Tanya Wilkins, product marketing manager at Mandiant. “That means organizations need out-of-band (OOB) communications and other ways to act quickly when the environment becomes inaccessible.”

OOB communications are separate, independent channels used by organizations to maintain coordination and communication when primary communication systems are unavailable or compromised, such as during a ransomware attack.

Fried emphasizes that threat intelligence functions must now play a more central role in preparedness: “We’re seeing organizations move toward joint response models that bring security operations, intel, and response together before a crisis happens.”

Planning for this complexity means going beyond technical defenses and building a response strategy that reflects today’s attacker behaviors and hybrid infrastructure realities. Many organizations now operate across on-premises data centers, multiple cloud providers, and third-party software-as-a-service platforms — each with different logging, access, and security models. Effective IRPs must account for this complexity and ensure visibility across all environments.

"Critical information such as contact details may be incorrect or outdated, and communication plans might be stale. Consequently, it is often unclear what criteria justifies invoking the incident response plan and who is authorized to do so."

Ryan Fried
Principal security consultant,
Mandiant

Organizations of all sizes struggle with incident response planning

Even organizations with mature security programs often struggle to create and maintain a usable IRP. A significant challenge is often ownership.

“When accountability is not clearly defined, the plan can fall into a state of neglect, becoming outdated or siloed,” says Fried. “Because rewriting the entire plan is a significant undertaking — requiring communication with stakeholders and incorporating insights across every process and role in the response lifecycle — the document is often updated only in fragmented sections, if at all.”

Another issue is complexity. In global organizations, varying regional structures can make it difficult to maintain a single, unified plan. “For example, a document that serves one branch in the Americas may not align with the operational realities of a branch in the Asia-Pacific region, making a centralized plan challenging to manage and implement,” Fried says.

Smaller businesses may believe that IR planning is out of reach. Without a CISO or dedicated security team, the work often falls to someone with limited capacity or expertise.

Yet even these organizations can start small and build from there.

The anatomy of an effective incident response plan

A strong IRP should be practical, tested, and tailored to your organization’s risk profile. Mandiant recommends including the following elements:

- **Executive sponsorship:** Executive leadership — such as the CISO, CTO, or CEO — must be visibly involved and ultimately accountable.
- **Defined severity levels:** IRPs should classify incidents according to severity level. These levels should be clearly defined to help teams understand urgency and priority and when escalation is required.
- **Lifecycle alignment:** Use frameworks such as NIST SP 800-61 or ISO 27035 to structure the IRP around the core phases of an incident: planning, detection, response, and recovery.
- **Incident response playbooks:** Develop playbooks for key scenarios like ransomware, insider threats, or cloud breaches. These documents standardize actions and accelerate decision-making.
- **Roles and responsibilities:** Utilize the responsible, accountable, consulted, and informed (RACI) model to define functional ownership across teams.
- **Communication plans:** Establish clear communication protocols that identify internal stakeholders (executives, IT, legal) and external parties (customers, regulators, insurers). Define how and when to communicate with each and OOB communications protocols.
- **Testing and revision:** Conduct regular tabletop exercises (covering a range of scenarios) to help test and assess your IRP. After each incident, perform a lessons-learned review to update the plan based on what worked and what didn’t.

Planning is not a one-time event. “It’s a constant process,” says Wilkins. "You need to continuously improve it and keep it fresh as people come and go and as your organization grows."

A minimum viable plan for small organizations

If you have limited resources, a basic plan is still far better than no plan.

“At a minimum, you need something that makes sense for the size of your organization, such as basic playbooks and a communications process,” Wilkins says. “You can always build on it.”

Fried recommends using the NIST framework as a starting point. “It’s a great way to start visualizing how to move forward, even without a complete plan. You can map your existing capabilities to those buckets and expand from there.”

Organizations can dramatically reduce the impact of a breach with modest capabilities, having clarity on who to call, what steps to take, and how to coordinate internal response.

The Mandiant Retainer advantage

When an incident occurs, every second counts. The Mandiant Retainer gives organizations immediate access to world-class expertise — and delivers significant value even before a breach occurs.

With a retainer in place, customers benefit from:

- **A two-hour response time:** Mandiant experts can be actively engaged within two hours of an incident being declared.
- **Proactive services:** Retainer units can be used for Mandiant services including tabletop exercises, red teaming, and playbook development.
- **Pre-established terms:** Legal, operational, and technical details are worked out in advance, accelerating response in a crisis.
- **Flexible redemption:** Clients can apply retainer units toward staff education, strategic consulting, or threat intelligence services to boost readiness.

Surfacing blind spots and risks early

“Many clients opt for a Mandiant Incident Response Preparedness Service (IRPS) while establishing or renewing their IR retainer,” says Jose Toledo, senior security consultant with Mandiant. During an IRPS engagement, consultants build a profile of the client’s environment by collecting data and holding a series of workshops. This helps Mandiant respond effectively upon an incident declaration and helps our customers learn what to expect upon activating a retainer.

“We examine their infrastructure, processes, and incident procedures to gain a comprehensive understanding and identify any gaps,” Toledo says. “Subsequently, we provide recommendations that enhance the organization’s ability to support an incident response engagement in the event of a security breach.”

> “We examine their infrastructure, processes, and incident procedures to gain a comprehensive understanding and identify any gaps.”
>
> **Jose Toledo**
> Senior security consultant,
> Mandiant

These assessments provide far more than documentation updates. For example, a review of an organization’s logging practices helps Mandiant understand its level of security visibility. Mandiant may recommend longer retention periods for certain log types or flag key monitoring gaps that could impede an investigation.

By surfacing blind spots and uncovering risks early, the assessment helps clients harden their environments and reduce incident response time when every second counts. “In some multi-cloud environments, we’ve discovered that certain logs weren’t being collected, or certain security tools weren’t enabled,” Toledo says.

A significant bottleneck that can hinder a quick incident response is the process of gaining access to security tools. IR consultants often face this challenge due to the lack of pre-approval for provisioning accounts for IR responders. Addressing this issue during the preparedness phase is essential for eliminating delays when an actual incident occurs.

Readiness is the real advantage

Cyber incidents are inevitable, but confusion and disorganization do not have to be. An effective, up-to-date incident response plan gives organizations the clarity, structure, and confidence to act decisively under pressure. It transforms a reactive posture into a proactive one.

With Mandiant as a trusted partner, organizations gain the benefit of two decades of frontline expertise, real-time threat intelligence, and tailored services to build resilience before the breach occurs. Mandiant's multi-cloud expertise helps organizations prepare for and respond to incidents across Google Cloud, Microsoft Azure, Amazon Web Services (AWS), and other environments.

Need help building, updating, or testing your IR plan? Discover how a Mandiant Retainer ensures you’re ready before a cyber incident or security breach — and supported when one occurs. Visit Mandiant to learn more.