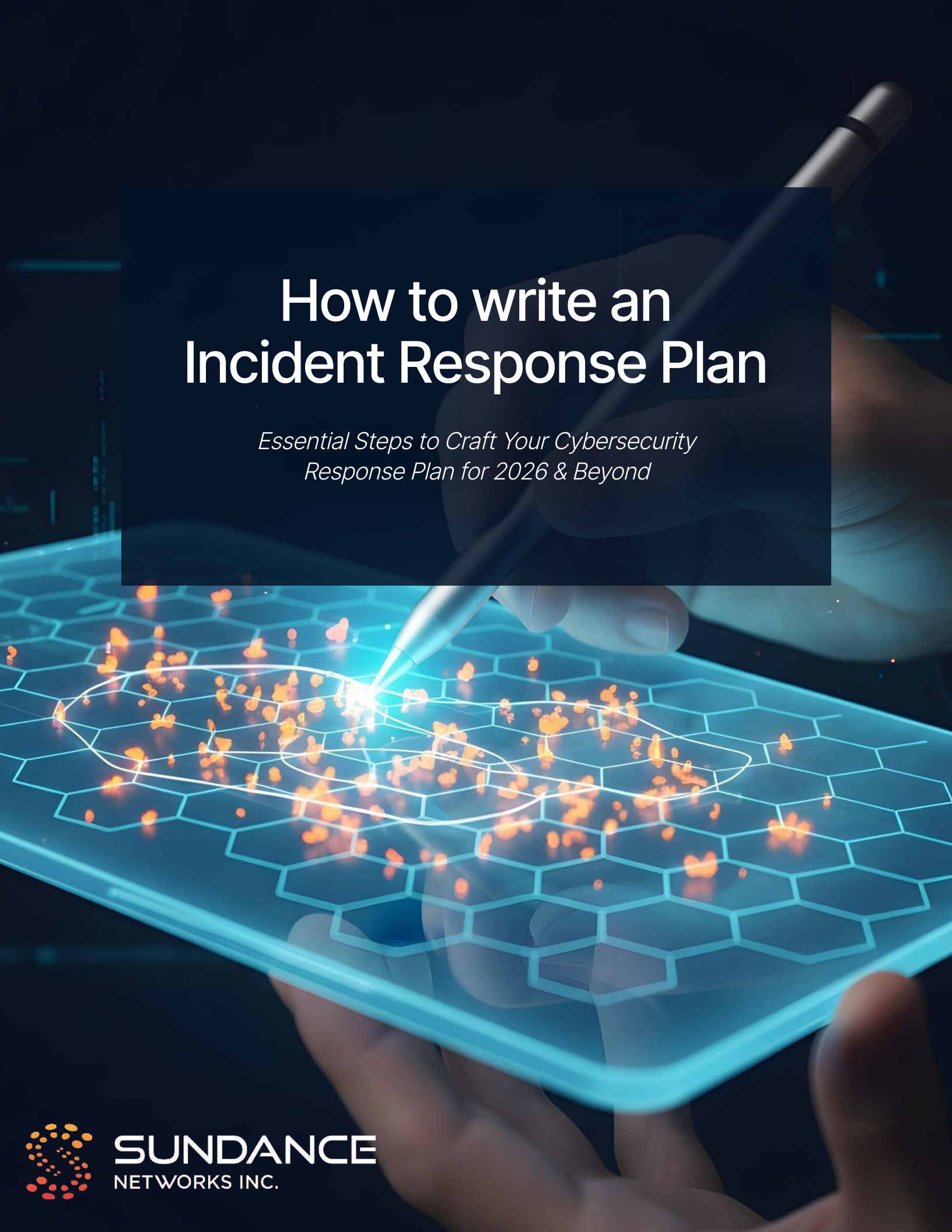


How to write an Incident Response Plan

Essential Steps to Craft Your Cybersecurity Response Plan for 2026 & Beyond

SUNDANCE NETWORKS INC.

The goal of an Incident Response Plan (IRP) is to help your organization respond to cybersecurity incidents calmly, quickly, and with minimal damage. Think of it as a fire drill — you hope you never need it, but it's critical to have a clear plan if something goes wrong.

Business Benefit: Limits financial loss, reputational damage, and compliance risks during a security incident.

Business-Focused Incident Response Plan Procedure

1. Assign Clear Roles and Responsibilities

List the people responsible during a cyber incident — even if you're a small team. Define who will:

- Lead the response effort
- Communicate with staff and customers
- Contact legal or regulatory bodies
- Work with IT or external vendors
- Document everything for review

Business Benefit: No panic or confusion when things go wrong — everyone knows exactly what to do.

2. Decide What "Counts" as an Incident

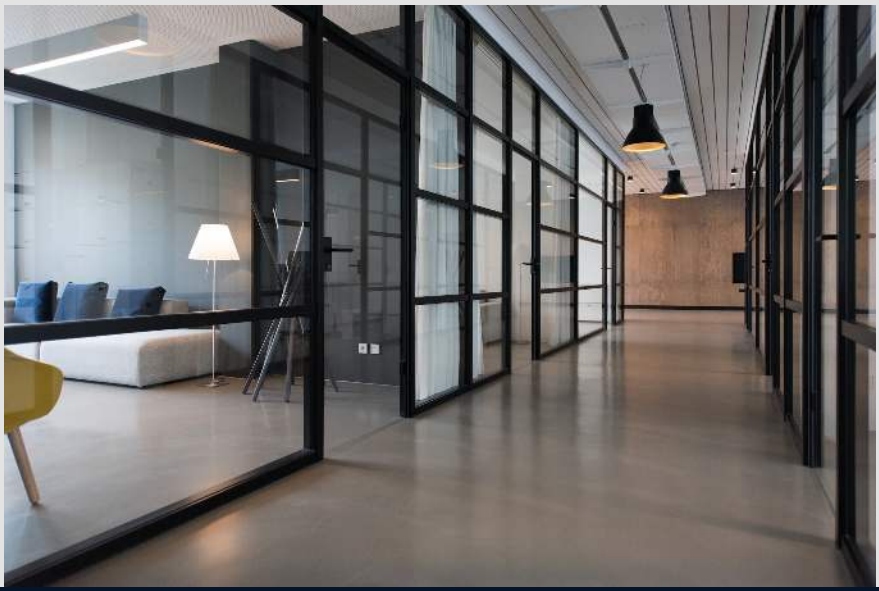
Not every warning or glitch is an emergency. Clarify:

- What types of issues are minor and monitored
- Which ones are serious and need action
- When something becomes a business-impacting incident

Examples:

- Spam email = Low risk
- Compromised login = Medium risk
- Data breach = High risk

Business Benefit: Helps you prioritize your response and avoid overreacting or underreacting.



3. Establish How Incidents Are Detected

Make a list of how issues are usually discovered. This could include:

- Employees noticing something strange
- Antivirus software or IT vendors alerting you
- Customers reporting suspicious activity

Business Benefit: Knowing your detection points helps you respond faster and plug gaps.

4. Create an Action Plan for Containment

If something bad happens (like a malware infection), what steps will you take to keep it from spreading?

Example actions:

- Disconnect affected devices from the internet
- Change passwords
- Notify your IT provider or MSP

Business Benefit: Prevents one small issue from becoming a company-wide disaster.

5. Detail How You'll Fix the Problem

Once it's contained, how will you remove the cause and return to business? This includes:

- Cleaning systems
- Replacing hardware if needed
- Restoring from backups

Business Benefit: Ensures you're not just putting out fires — you're solving the root cause.

6. Plan for Business Recovery

List how you'll get back to normal operations. This could include:

- Restoring data
- Bringing systems back online
- Verifying everything is safe

Business Benefit: Reduces downtime and loss of productivity.

7. Prepare a Communication Strategy

Decide who you'll notify and how:

- Staff (What should they do?)
- Clients (What happened and what are you doing about it?)
- Regulators (if sensitive data is involved)
- Public (if media attention is likely)

Business Benefit: Protects your brand's reputation with clear, honest communication.

8. Review and Learn from Each Incident

After the incident, schedule a short review meeting.

Discuss:

- What worked and what didn't
- What should change in the plan
- What can be done to prevent it from happening again

Business Benefit: Turns a bad experience into a growth opportunity for your team and operations.

9. Test the Plan Every 6–12 Months

Just like a fire drill, test your response plan regularly. Simulate a cyberattack and walk through the plan with your team.

Business Benefit: Builds confidence, accountability, and helps uncover any blind spots.

10 Tips to Avoid Needing an Incident Response Plan

- 1. Use multi-factor authentication (MFA) everywhere.
- 2. Update all software and systems regularly.
- 3. Backup your data daily, both on-site and in the cloud.
- 4. Train employees on phishing and password safety.
- 5. Use strong antivirus/antimalware tools.
- 6. Don’t allow employees to use personal devices for work without controls.
- 7. Have a clear employee offboarding process.
- 8. Limit access to sensitive information based on role.
- 9. Monitor accounts and systems for unusual behavior.
- 10. Work with a trusted Managed Service Provider (MSP) for proactive protection.

Ready to Create Your Plan?

Don't let a cyber incident catch you unprepared. Contact Sundance Networks today to build a customized Incident Response Plan that protects your business, minimizes damage, and keeps operations running when it matters most. Reach out now for a free consultation and discover how a solid Incident Response Plan can be the difference between a minor disruption and a business-threatening disaster.

Contact Sundance Networks Today

Sundance Networks

Sundance Networks has provided expert IT support since 2003, helping hundreds of businesses increase productivity and profitability by making IT a streamlined part of operations. Our mission is to deliver the latest technology Managed IT Services, Business Continuity. VoIP Services, Cloud Services, and Security Services as a highly cost-effective IT solution in order to maximize our clients' productivity and profitability.