Office Hours, March 4, 2026

Cyber Security Resources

Resources for Developing an Incident Response Plan for a Small Business

Small businesses don't need an enterprise-scale security program to build an effective incident response plan, but they do need clear guidance, realistic expectations, and practical templates. The resources below are widely used, credible, and well suited for organizations with limited staff and budget.

Government and Public-Sector Resources

CISA's Small and Medium Business Cybersecurity Resources are among the most practical free materials available. They are written specifically for small and mid-sized organizations and include guidance on incident response planning, roles and responsibilities, and ransomware preparedness. The material is designed to be approachable for non-specialists and works well as a foundation for a first incident response plan.

NIST's Small Business Cybersecurity Corner provides guidance on responding to cyber incidents without requiring deep familiarity with NIST frameworks. It includes plain-language explanations of what to do after an incident and links to more detailed standards for organizations that want to go deeper.

NIST Special Publication 800-61 Revision 3, released in April 2025, is the authoritative U.S. incident response guide. While it is comprehensive, it is explicitly designed to be scalable. Small businesses typically adapt it by simplifying roles, reducing documentation depth, and focusing on the most likely incident types such as phishing, ransomware, and account compromise.

Practical Templates and Starter Guides

The Cybersecurity Nonprofit (CSNP) Incident Response Plan Template is a strong starting point for small businesses and nonprofits. It includes defined team roles, communication checklists, and legal considerations, making it easy to customize without starting from a blank page.

PurpleSec's incident response guide for small businesses explains the incident response lifecycle in plain language and walks through what a plan should contain. It's particularly useful for business owners or IT managers writing their first plan.

CloudGuard's incident response plan guide focuses on common small-business questions such as after-hours incidents, who to call first, and how to avoid decision paralysis. It is written from an operational perspective rather than a compliance one.

Policy and Framework Templates

The SANS Institute provides free policy templates, including incident handling and response documents. These are more structured and formal, but many small businesses successfully trim them down to fit their size while keeping the core concepts intact.

A commonly used SANS-derived incident response template in PDF format provides a traditional written plan with objectives, roles, and response phases already defined. This is helpful for organizations that need a formal document for insurance, audits, or customer requirements.

Reporting and External Support Resources

The FBI's Internet Crime Complaint Center (IC3) is the primary federal reporting mechanism for cybercrime. Small businesses should include IC3 reporting as a step in their incident response plan, especially for fraud, business email compromise, and ransomware incidents.

The Federal Trade Commission's cybersecurity guidance for small businesses complements an incident response plan by addressing recovery steps, customer notification considerations, and basic security hygiene that reduces repeat incidents.

How Small Businesses Typically Use These Resources

Most small businesses build an effective incident response plan by starting with CISA or CSNP materials for structure, borrowing simplified concepts from NIST 800-61, adapting a template instead of writing from scratch, and clearly defining who to call, what systems to isolate, and how to communicate internally and externally.

The goal is not perfection or exhaustive documentation. The goal is clarity, speed, and confidence when something goes wrong.

If you'd like, I can help you turn one of these into a tailored incident response plan, create a one-page "what to do first" checklist, map common incidents like ransomware or business email compromise to response steps, or rewrite an incident response plan so it's usable by non-technical staff and leadership.