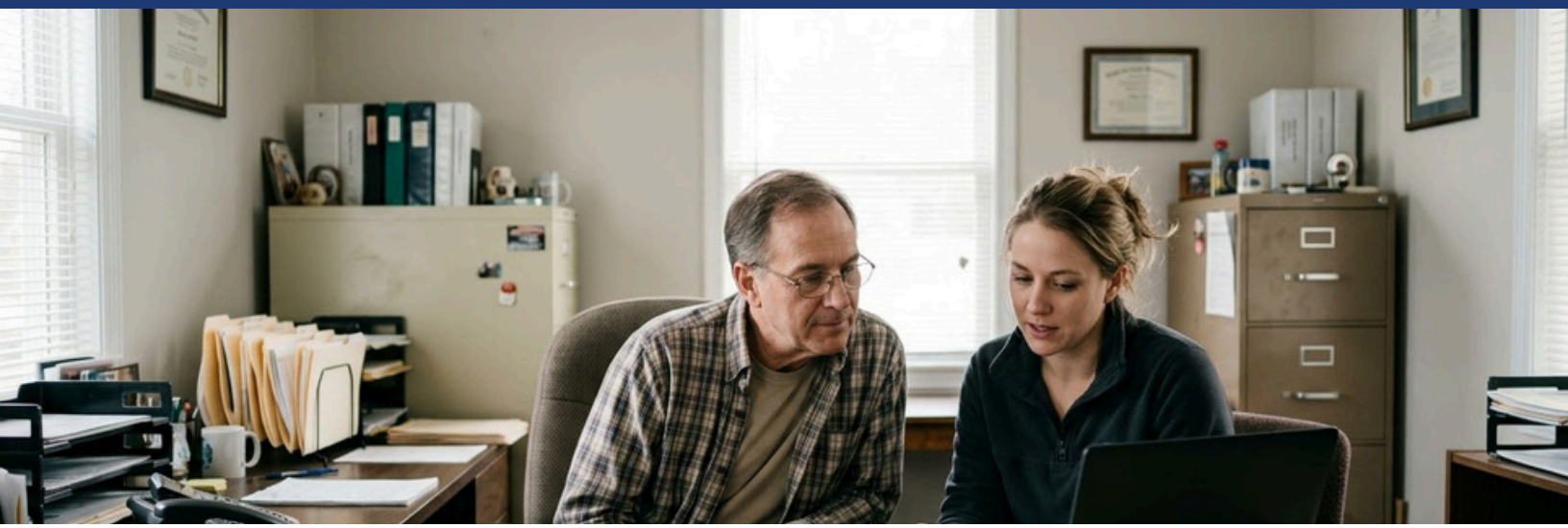
SJBA
South Jersey Business Association

BUSINESS PLANNING SERIES · WORKBOOK 08

Coordinate the Response. Restore Operations Carefully.

Cybersecurity Incident Recovery Coordination Workbook



This is an owner-level coordination tool, not a forensic or technical manual. It helps you engage qualified help, separate facts from unknowns, record decisions and evidence handoffs, and verify recovery under specialist direction.

INSIDE THIS WORKBOOK

02 First steps: coordinate before acting
03 Confirmed observations versus unknowns
04 Incident contacts and decision authority
05 Critical-process and dependency map
06 Evidence-preservation request and handoff log
07 Containment and assessment coordination record
08 Business continuity worksheet
09 Personal-information exposure checkpoint
10 Recovery plan and validation
11 Communication approval log
12 Expense, impact, decision, and retention log
13 Specialist-led lessons learned and action plan
14 Official sources, About SJBA, and next steps

02 · IMMEDIATE COORDINATION

First steps: coordinate before acting

Unverified actions can destroy evidence or make recovery harder. Engage qualified help first.

Safety first

If anyone is in physical danger, call 911. Follow qualified incident-response direction before deleting files, wiping devices, or restoring systems. This workbook does not tell you to shut down or disconnect anything; your specialist decides.

COORDINATION CHECKLIST

- [ ] Contact qualified incident-response support
- [ ] Contact qualified legal counsel
- [ ] Avoid unapproved changes to affected systems
- [ ] Use a trusted communication channel
- [ ] Check whether your insurance policy covers cyber incidents
- [ ] Record times and observations as they happen

Incident-response provider	Contacted (date and time)	Contacted by

NOTES

03 · FACTS AND UNKNOWNS

Confirmed observations versus unknowns

Record what was observed, by whom, and whether a professional has verified it. Keep guesses out of the facts column.

Time and time zone	Source	Observed effect	Business activity affected	Reported by	Verified?

Open unknowns

NOTES

04 · CONTACTS AND AUTHORITY

Incident contacts and decision authority

Agree who decides what. Record contact methods, not credentials.

No passwords or recovery codes

Do not write passwords, recovery codes, or access keys anywhere in this workbook.

Role	Name	Trusted contact method	Authority to decide	Engaged (time)
Business decision lead				
Technical incident lead				
Legal counsel				
Insurer or broker				
IT provider				
Communications lead				
Law enforcement contact, if engaged				



05 · CRITICAL PROCESSES

Critical-process and dependency map

Map the incident at the business level: what work is affected and what it relies on.

Business process	Systems relied on	Priority 1–3	Owner	Approved workaround	Uncertainty

06 · EVIDENCE HANDOFFS

Evidence-preservation request and handoff log

Your specialist directs evidence collection. Record requests and handoffs; reference secure locations, not contents.

Request	Requested by	Handling authority	Timestamp (time zone)	Secure location reference	Follow-up

07 · CONTAINMENT

Containment and assessment coordination record

Separate proposed, approved, and completed actions. Each action should be directed by your specialist and approved by the business lead.

Action	Proposed by	Approved by	Status	Date and time	Notes

Status: proposed, approved, in progress, completed, or declined.

08 · CONTINUITY

Business continuity worksheet

Decide how essential work continues while systems are affected, using lawful, approved alternatives.

Service	Approved manual alternative	Service limits	Customer obligations to review	Cash impact	Owner

Controls on manual workarounds (approvals, records, payment verification)

NOTES

09 · LEGAL ASSESSMENT

Personal-information exposure checkpoint

An incident may or may not involve personal information. Qualified counsel assesses obligations and timing.

Counsel determines obligations

New Jersey and other states, along with some federal rules and contracts, may require notifications when certain personal information is involved. Do not assume a deadline applies or that no breach occurred until counsel has assessed verified findings.

Responsible professional

Assessment date

Question	Verified finding	Source	Next decision
Was personal information involved?			
What types?			
Whose information?			
Which states or jurisdictions?			
Contract obligations to customers or partners?			
Regulatory obligations to assess?			

NOTES

10 · RECOVERY

Recovery plan and validation

Restore from sources your specialist has approved. Do not assume backups are clean.

System	Approved restoration source	Professional checks	Dependencies	Authorized by	Rollback criteria

VALIDATION QUESTIONS FOR YOUR SPECIALIST

1 How will we know a restored system is safe to use?

2 What monitoring will continue after recovery, and for how long?

NOTES

11 · COMMUNICATION

Communication approval log

Share only verified facts, through approved channels, after qualified review. No pre-written notifications are included.

Audience	Verified facts to share	Reviewed by counsel	Channel	Owner	Sent and next update
Staff					
Customers					
Partners and vendors					
Insurer					
Regulators, if counsel advises					
Media inquiries					

NOTES

12 · RECORDS

Expense, impact, decision, and retention log

Keep a running record with secure references rather than sensitive evidence.

EXPENSES AND SERVICE IMPACT

Date	Item	Amount	Category	Secure reference

DECISIONS AND RETENTION

Date	Decision	Decided by	Retention instruction	Reference

13 · LESSONS AND ACTIONS

Specialist-led lessons learned and action plan

Review with your specialist once operations are stable. No plan guarantees complete security.

REVIEW QUESTIONS

1 What helped the response, and what slowed it down?

2 Which improvements did the specialist recommend, and how will each be validated?

3 What will change in our contacts, backups, access, and training?

ROLES THAT MAY BE RELEVANT

- ☐ Incident-response firm
- ☐ Managed IT provider
- ☐ Privacy or cyber attorney
- ☐ Insurance broker
- ☐ Accountant
- ☐ Communications professional

PRIORITY ACTIONS

#	Action	Owner	Due	Depends on	Done
1					
2					
3					
4					
5					
6					

Review cadence: _____ Next review date: _____ Visit SJBA to explore current professionals.

NOTES

14 · SOURCES AND NEXT STEPS

Official sources, About SJBA, and next steps

OFFICIAL SOURCES, CHECKED OCTOBER 2026

CISA
Federal cybersecurity guidance for organizations, including small businesses.
www.cisa.gov

CISA: Report an incident
How organizations report cyber incidents to the federal government.
www.cisa.gov/report

New Jersey Cybersecurity and Communications Integration Cell
New Jersey's cybersecurity information sharing and incident reporting resource.
www.cyber.nj.gov

FBI Internet Crime Complaint Center (IC3)
Federal channel to report internet-enabled crime.
www.ic3.gov

FTC: Data Breach Response, A Guide for Business
Federal guidance on responding when personal information may be exposed.
www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

NIST Cybersecurity Framework
Federal framework for managing cybersecurity risk, including recovery.
www.nist.gov/cyberframework

Companion article: "Recovering From a Cybersecurity Incident." Find it with SJBA's business resources at southjerseybusinessassociation.org.

About SJBA

Founded in 1994, the South Jersey Business Association is a structured, category-exclusive referral network for South Jersey business owners serving Camden, Gloucester, and Burlington counties. Members hold one seat per professional category and follow attendance and referral standards.

Visit SJBA to explore current professionals

Established business owner? Visit a Meeting

Planning note. This workbook is general educational planning information for South Jersey business owners. It is not individualized legal, cybersecurity, insurance, or technical advice. Requirements vary by municipality, industry, and business; qualified professionals and the relevant authorities should confirm applicable decisions. SJBA does not perform, supervise, or guarantee the work of any member or other professional. Rules change; confirm details with each source. Photos are illustrative, not SJBA members or member projects.