

The Small Business Cybersecurity Check-Up: 10 Things to Fix This Week

Michelle Bufano, Esq. | Webinar takeaway checklist

Review the same ten items covered in the webinar. Mark each Done, Needs work or Not sure. Choose three priorities and assign an owner and deadline. Address a suspected compromise immediately.

Part 1 Lowering your risk

1. Passwords and account access Require MFA, especially for email, banking and administrator accounts. Use unique passwords and a password manager. Remove former staff and unnecessary privileges. Prefer phishing-resistant MFA where available.

Status: Done / Needs work / Not sure

2. Devices, data and backups Update devices and software. Lock and encrypt devices, restrict sensitive sharing and retain records as required. Confirm vendor responsibilities for security and incident notice. Protect backups separately and test restoration; cloud synchronization alone may not be enough.

Status: Done / Needs work / Not sure

3. Staff reporting and payment checks Give everyone a clear reporting contact for suspicious activity and mistakes. Verify changed payment instructions through a known phone number. Practice a suspicious email with staff and contractors.

Status: Done / Needs work / Not sure

Your three priorities this week

Item ____ Action _____

Owner _____ Due _____

Item ____ Action _____

Owner _____ Due _____

Item ____ Action _____

Owner _____ Due _____

Keep these contacts available offline

Lead _____ Backup _____

IT _____ Counsel _____

Insurer _____ Bank _____

Alternate communication channel _____

Part 2 Readiness for a breach

Fix these response arrangements this week. During an incident, actions may overlap, especially bank contact, containment and preservation. Do not wait for certainty to get help.

4. Response leadership and contacts Name a response lead and backup. Keep IT, incident specialists, counsel, insurer and bank contacts offline. Check insurance reporting and provider requirements. If money moved, call the bank immediately and report fraud at ic3.gov.

Status: Done / Needs work / Not sure

5. Containment instructions Identify who can disconnect an infected device, revoke compromised sessions and pause payments. Use trusted devices and channels. Get expert help; avoid wiping, reinstalling or routinely powering down equipment before advice.

Status: Done / Needs work / Not sure

6. Evidence preservation Keep original messages, alerts and payment records. Record discovery time, facts and actions. Ask specialists to preserve logs before they expire. Screenshots supplement original records. Coordinate preservation with urgent containment.

Status: Done / Needs work / Not sure

7. Investigation responsibilities Confirm which specialist will assess affected accounts, devices, dates, information and people. Separate confirmed facts from unknowns. A lack of evidence of download does not establish that no information was exposed.

Status: Done / Needs work / Not sure

8. Notification requirements Locate client and vendor notice clauses and insurance instructions now. Assign counsel to assess applicable law and deadlines promptly if an incident occurs. Do not assume a universal deadline or wait for a final investigation report.

Status: Done / Needs work / Not sure

9. Communication procedures Choose a spokesperson and an alternate communication channel. Share verified facts, protective steps and the next update time. Avoid unsupported assurances. An urgent fraud warning may not satisfy formal breach-notice requirements.

Status: Done / Needs work / Not sure

10. Safe recovery and follow-through Plan safe workarounds and recovery priorities. Have specialists address the cause, validate backups and test restored functions before restart. Monitor afterward. Complete remaining notice duties, record lessons and assign corrective actions.

Status: Done / Needs work / Not sure

Free resources

NIST: nist.gov/itl/smallbusinesscyber

FTC: ftc.gov/business-guidance/resources/data-breach-response-guide-business

CISA: cisa.gov/stopransomware/ransomware-guide | FBI: ic3.gov