2W TECH
2W Technologies, INC

Cybersecurity Awareness Month - 2026
Week 4: How Organizations Build Resilience

Cyber Resilience Planning Checklist for 2027

Cyber resilience isn't about eliminating every risk. It's about making sure your organization can prevent what it can, respond when something goes wrong, recover quickly, and keep the business moving. Use this checklist to identify where your organization is prepared today and where to focus in 2027.

1 Governance & Leadership

Cybersecurity is a business responsibility. Leadership sets the tone, defines ownership, and ensures the organization is prepared.

- ☐ **Establish clear cybersecurity ownership**
  Define who is accountable, who makes decisions, and when issues escalate to leadership.
- ☐ **Define roles before an incident**
  Assign responsibilities for technical response, business continuity, communications, legal/compliance, and vendor coordination.
- ☐ **Make cybersecurity part of business planning**
  Consider cyber risk when adding new technology, working with vendors, completing acquisitions, or expanding operations.
- ☐ **Review cybersecurity risk with leadership regularly**
  Discuss key risks, progress on remediation, and changes in the threat environment.

2 Employees & Security Awareness

Your people are a critical part of your defense. Ongoing training and clear guidance help reduce risk and improve response.

- ☐ **Provide ongoing security awareness training**
  Focus on real-world threats like phishing, social engineering, MFA fatigue, and impersonation.
- ☐ **Prepare employees for AI-enabled threats**
  Include guidance on AI-generated content, voice impersonation, and risks associated with unapproved AI tools.
- ☐ **Make reporting suspicious activity easy**
  Ensure employees know what to report, how to report it, and what to do if they've already engaged.
- ☐ **Test awareness**
  Use phishing simulations, scenario-based training, or tabletop exercises to see how people actually respond.

3 Resilience & Recovery

Assume something will eventually go wrong. Be ready to respond and recover so your business can keep moving.

- ☐ **Identify what the business cannot operate without**
  Determine your most critical systems, data, processes and vendors.
- ☐ **Review your backups**
  Confirm what is being backed up, how it's protected, who can access it, and how quickly it can be restored.
- ☐ **Actually test recovery**
  Don't just have backups — prove they work.
- ☐ **Build or update your incident response plan**
  Document roles, decision-making, communications and escalation processes.
- ☐ **Run a tabletop exercise**
  Walk through realistic scenarios with leadership to test your plan and identify gaps.

4 Emerging Risks

The threat landscape is always evolving. Keep these areas on your radar as you plan for the year ahead.

- ☐ **AI use**
  Understand what AI tools are being used, what company information is entered into them, and whether governance is in place.
- ☐ **Identity and access**
  Ensure MFA is consistently deployed, privileged accounts are controlled, and inactive accounts are removed.
- ☐ **Third-party risk**
  Identify which vendors have access to your systems or data and assess how they're monitored.
- ☐ **Technology change**
  Evaluate the risks and dependencies introduced by new software, integrations, and automation.

5 Questions Every Executive Team Should Ask Annually

Use these questions to guide a meaningful conversation about your organization's cybersecurity readiness.

- ☐ 1. What are the three systems or processes we cannot operate without?
- ☐ 2. If one went offline tomorrow, how long could we function without it?
- ☐ 3. When did we last test restoring our critical systems and data?
- ☐ 4. What are our biggest cybersecurity risks right now?
- ☐ 5. What changed in our technology environment over the past year?
- ☐ 6. Who has access to our most sensitive systems and information?
- ☐ 7. Which third parties create meaningful cybersecurity dependencies for us?
- ☐ 8. Do we know what employees are doing with AI and company data?
- ☐ 9. If we had a major incident tomorrow, does everyone know their role?
- ☐ 10. When did we last test our response instead of simply reviewing the plan?
- ☐ 11. If we couldn't prevent the next incident, are we confident we could recover from it?

YOUR 2027 ROADMAP

