# Business Risk Readiness Scenario Workbook

Walk through each scenario to evaluate your organization’s readiness, response plan, and mitigation options.

## Scenario 1: POS Compromise (Retail)

☐ Is your POS network segmented from public Wi-Fi?
☐ Are your POS systems encrypted and up to date?
☐ Who would you call if card data was stolen?
☐ Do you have a plan for communicating a breach to customers?

## Scenario 2: Payroll Phishing (Food Service)

☐ Do you require MFA for payroll system access?
☐ Are change requests double-verified verbally or in-person?
☐ Who has access to change payroll settings?
☐ How quickly would you catch unauthorized changes?

## Scenario 3: Ransomware Outbreak (Manufacturing)

☐ Are backups offsite and tested regularly?
☐ How fast can you rebuild critical systems?
☐ Do staff know how to recognize phishing attempts?
☐ Would you pay the ransom—or have a recovery plan?

## Response Planning

☐ Who leads incident response?
☐ Who do you notify (law enforcement, clients, vendors)?
☐ Do you have cyber liability insurance?
☐ Have you tested your response plan with a tabletop exercise?