After Action Review (AAR)

Retail Holiday Season Attack Simulation

Exercise Scenario: Simulated Ransomware Attack During Holiday Season
Date Conducted: November 2025
Participants: Executive Team, IT Operations, Customer Service

Executive Summary
This After Action Review documents the organization's response to a simulated ransomware attack targeting point-of-sale systems and customer databases during peak holiday shopping season. The exercise revealed both strengths and areas requiring immediate improvement in incident response procedures.

Scenario Overview
At 2:00 AM EST, intrusion detection systems identified suspicious lateral movement across the network. By 2:45 AM, systems began displaying ransom demands. The attack targeted payment card data and customer personal information. Response team was activated per incident response plan.

Key Findings
What Went Well:
✓ Executive notification occurred within 15 minutes of detection
✓ Backup systems were isolated immediately, preventing additional data loss
✓ Customer communication protocol was activated within 45 minutes
✓ Board notification completed within 2 hours
✓ Law firm and cyber insurance carrier engaged appropriately

Areas for Improvement:
■ Initial triage took 20 minutes to determine scope (target: 10 minutes)
■ Incident response playbook was not immediately accessible to all participants
■ Communication between IT and executive team could be streamlined
■ Vendor notification procedures need clarification

Recommendations
1. Establish real-time incident command center with pre-defined roles and escalation paths
2. Conduct quarterly incident response drills focused on speed of initial response
3. Develop communication templates for customer, board, and regulatory notifications
4. Implement automated systems health checks to accelerate damage assessment
5. Verify backup restoration procedures are tested monthly

Next Steps
• Update incident response procedures (by January 15)
• Conduct leadership training on response protocols (January)
• Implement backup verification automation (February)
• Schedule follow-up tabletop exercise (Q2 2026)

Conclusion
The organization demonstrated solid foundational incident response capabilities. With the recommended improvements, response time and decision-making clarity will be significantly enhanced, reducing potential business impact from future security incidents.

AAR Generated: June 18, 2026
Document prepared by CyberShield Technologies