KixxByKyee Incident Response Playbook

# 1. Purpose & Scope

This playbook outlines how KixxByKyee (a sneaker resell company) detects, contains, eradicates, and recovers from cybersecurity incidents. It ensures business continuity, protects customer data, and maintains compliance with applicable laws.

# 2. Roles & Responsibilities

- Incident Response Lead (IRL): Coordinates all IR activities and decision-making.  
- IT/Security Team: Conducts detection, containment, and eradication.  
- Business Owner: Authorizes recovery actions and communications.  
- All Employees: Report suspicious activity immediately.

# 3. Incident Categories & Examples

- Malware Infection (trojans, spyware).  
- Phishing Attack (fake sneaker drops targeting employees).  
- Denial of Service (DoS/DDoS) (bot attacks on sneaker release day).  
- Ransomware (files locked, payment demanded).

# 4. Detection & Analysis

Methods:  
- Review system logs (failed logins, unusual activity).  
- Monitor suspicious emails (phishing attempts).  
- Customer complaints (slow website, failed checkout).  
  
Example Detection Rule:  
Multiple failed login attempts from the same IP within 5 minutes triggers an incident alert.

# 5. Containment Strategy

- Short-term containment: Disable compromised accounts, isolate infected devices from the sneaker ordering system.  
- Long-term containment: Apply firewall rules, block malicious IP addresses, update access permissions.

# 6. Eradication & Recovery

- Eradication: Remove malware, patch vulnerabilities, reset passwords.  
- Recovery:  
 • Restore from secure backups.  
 • Validate sneaker transaction system is working properly.  
 • Reconnect affected devices after confirming clean state.

# 7. Evidence Preservation

- Maintain chain of custody for all logs and files.  
- Save email headers, system logs, and forensic images if possible.  
- Document each step in the incident ticketing log.

# 8. Communication Plan

- Internal Notification: IRL informs staff via email or chat.  
- External Notification: Customers are notified if data is compromised.  
- Legal Reporting: Notify regulators if required under CT privacy laws (CTDPA).

# 9. Post-Incident Activities

- Root Cause Analysis (RCA): Identify vulnerabilities and how attackers exploited them.  
- Lessons Learned Meeting: Update playbook with new detection/response measures.  
- Policy Improvement: Update security policies to prevent recurrence.

# 10. Legal & Ethical Compliance

Relevant Laws:  
- CT Data Privacy Act (CTDPA) – governs customer personal data.  
- FTC Safeguards Rule – requires businesses to protect sensitive information.  
  
Ethical Considerations:  
- Transparency with customers about breaches.  
- Protecting sneaker buyers’ financial data.

# 11. CIA Triad Mapping

- Confidentiality: Customer payment data encrypted with TLS 1.2+ in transit and AES-256 at rest.  
- Integrity: Log monitoring ensures sneaker inventory and sales records are accurate.  
- Availability: Backups and DoS protections ensure sneaker drops run smoothly.

# 12. Incident Tracking Table (Example)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident Type | Detection Method | Containment Action | Recovery Action | Status |
| Phishing Email | Employee reports suspicious email | Block sender domain | Train staff | Closed |
| Malware Infection | Log shows unusual process | Isolate infected laptop | Restore from backup | Resolved |
| DoS Attack | Website slowdown detected | Block IPs via firewall | Scale servers | Mitigated |

# Appendix A – TLS 1.2+ and AES-256 Diagram

The diagram below supports the Incident Response Playbook by showing encryption methods used in both transit and storage.