THE ASSUME BREACH PLAYBOOK

Executive Summary | Critical Incident Response Protocol

Executive Overview: This playbook provides immediate action steps for leadership when a cybersecurity breach is suspected or confirmed. Time is critical—every minute counts in containing the threat, preserving evidence, and protecting organizational assets. Follow these protocols in sequence to minimize damage and ensure coordinated response.

SECTION 1: ISOLATE THE INFECTED DEVICE

Immediate Actions (Within 5 Minutes):

• **Physical Disconnection:** Immediately disconnect the affected device from all networks—unplug ethernet cables and disable Wi-Fi/Bluetooth. Do NOT shut down the device as this may destroy volatile evidence in RAM.

• **Quarantine Connected Systems:** Identify and isolate any systems that had recent communication with the infected device. Review network logs, shared drives, and active sessions to determine the blast radius.

• **Preserve Evidence:** Do not delete files, clear logs, or modify system configurations. Take photographs of error messages and unusual behavior. Document the timeline of events and initial observations.

• **Account Lockdown:** Immediately disable user credentials associated with the compromised device. Reset passwords for any accounts that were accessed from the device within the past 48 hours.

SECTION 2: ACTIVATE THE INCIDENT RESPONSE TEAM

Critical Stakeholder Activation (Within 15 Minutes):

• **Internal Response Team:** Convene the core incident response team including CISO/CIO, IT Security Lead, Network Administrator, and Executive Sponsor. Establish a dedicated war room (physical or virtual) for coordination.

• **Legal Counsel Engagement:** Immediately notify General Counsel and outside cybersecurity legal counsel. Legal guidance is essential for privilege protection, regulatory compliance, and breach notification obligations under GDPR, CCPA, HIPAA, or other applicable frameworks.

• **Forensics and External Support:** Contact pre-approved digital forensics firm and cyber insurance carrier. Preserve attorney-client privilege by routing all external engagement through legal counsel to ensure investigation findings remain protected.

• **Executive Notification:** Brief CEO, Board, and relevant C-suite executives on situation status, containment measures, and potential business impact. Prepare for rapid decision-making on resource allocation and public disclosure.

SECTION 3: COMMUNICATION PROTOCOL

■ CRITICAL: DO NOT USE EMAIL OR COMPROMISED SYSTEMS ■

• **Approved Communication Channels:** Use only secure, out-of-band communication methods: Personal mobile phones (voice calls only), Signal or WhatsApp encrypted messaging, or in-person meetings. Assume all corporate email, Slack, Teams, and internal networks are compromised.

• **Contact Hierarchy & Escalation:** Primary: Direct phone calls to IRT members. Secondary: Encrypted messaging apps with verified contacts. Tertiary: Physical assembly at predetermined secure location. Maintain updated contact cards with personal mobile numbers for all critical personnel.

• **Information Control:** Limit initial communications to essential personnel only. Use code names or generic terms ('IT incident') until legal counsel approves specific disclosure. Do not discuss technical details or attribution over unsecured channels.

• **Documentation Protocol:** Maintain handwritten incident logs in a secure physical location or use encrypted note-taking tools on non-networked devices. All documentation should be treated as potentially discoverable in litigation—consult legal counsel before creating records.

Alternative Communication Decision Tree:

Need to communicate?
↓
Can you meet in person?
YES → In-person meeting | NO → ↓
Is it urgent (<15 min)?
YES → Personal mobile call | NO → ↓
Use Signal/WhatsApp encrypted messaging

Sample Initial Message Template:

"This is [Your Name]. We have a critical IT incident requiring immediate IRT activation. Do NOT use email or corporate systems. Call me directly at [personal mobile] within 5 minutes. This is time-sensitive and requires secure communication only."

NEXT STEPS: Once the IRT is assembled and secure communications are established, proceed to full incident response procedures including threat assessment, containment strategy, eradication planning, and recovery operations. Legal counsel will guide breach notification requirements and regulatory compliance obligations.