Create an Incident Response Checklist for a Small Business

📋 BrightTech Solutions Incident Response Checklist

1️⃣ Preparation

- **Identify Critical Assets**
    - Customer databases
    - Ongoing project files
    - Financial records
    - Employee workstations
- **Assemble Incident Response Team**
    - IT Manager: Lead and coordinate response
    - System Administrator: Isolate and analyze affected systems
    - Security Analyst: Investigate attack vectors and logs
    - Communications Officer: Manage internal/external communication
    - Legal Advisor: Handle legal obligations and regulatory reporting
- **Baseline Security Measures**
    - Enforce strong, regularly updated passwords
    - Implement antivirus with real-time protection
    - Set up isolated, offline backup storage
    - Security awareness training for employees
    - Email attachment filtering and sandboxing

2️⃣ Detection

- **Type of Attack:** Ransomware via phishing email attachment
- **Cause:** Employee opened malicious email attachment: *Urgent_Invoice.pdf*
- **Detection Time:** 8:00 AM when files became inaccessible
- **Detection Tools/Logs**
  - Email server logs
  - Antivirus alert logs
  - Network activity logs
  - File access audit logs
- **Systems Affected**
  - 15 workstations
  - Shared network drive (customer data, project files)
- **Business Impact**
  - All projects halted
  - Customer support inaccessible
  - Financial losses from downtime
  - Damage to trust and reputation

3️⃣ Containment

- **Immediate Actions**
  - IT Manager disconnects network (done at 8:15 AM)
  - Disable affected user accounts
  - Isolate infected systems physically/logically
  - Inform staff to avoid opening suspicious emails

- **Disconnection Decision**
  - Affected systems disconnected from network immediately
- **Shared Resources Management**
  - Disable shared drives access until cleaned and secured
- **Protect Unaffected Systems**
  - Verify security status of unaffected devices
  - Update antivirus definitions
  - Block further spread through firewall and endpoint protection
- **Business Continuity**
  - Set up temporary communication channels
  - Prioritize restoration of critical business services

4️⃣Eradication

- **Removal Steps**
  - Use ransomware removal tools (e.g., Malwarebytes Anti-Ransomware)
  - Wipe and reinstall OS on affected workstations if necessary
  - Scan network storage for malware remnants
- **Patch Vulnerabilities**
  - Update all antivirus software
  - Enforce password policies
  - Patch operating systems and software
  - Implement email attachment scanning policies

5️⃣Recovery

- **Restoration Without Ransom Payment**
  - Identify clean backups (verify integrity)
  - Restore essential data from secure offline backups
- **Verification Process**
  - Perform integrity checks on restored systems
  - Run antivirus/malware scans before reconnecting to the network
  - Monitor systems for anomalies
- **Testing**
  - Conduct system functionality tests
  - Confirm operational readiness of customer support systems
  - Test network drives and project file accessibility

6️⃣ Post-Incident Analysis

- **Lessons Learned**
  - Identify security gaps (weak password policy, no attachment filtering, no isolated backups)
  - Assess response effectiveness (containment and recovery speed)
- **Policy & Process Updates**
  - Implement mandatory cybersecurity training
  - Enforce stronger password policies
  - Isolate backup storage off the live network
  - Regular phishing simulations
  - Develop a formal incident response plan

📌 Tailored Recommendations for BrightTech Solutions

Ransomware Incident Response & Prevention

🔒 Immediate Security Improvements

1. **Strengthen Email Security**
   - Implement advanced email filtering for attachments and links.
   - Deploy sandboxing for suspicious attachments (e.g. PDFs, executables).
   - Enforce automatic flagging of external emails.
2. **Enforce Strong Password Policies**
   - Require complex, unique passwords.
   - Mandate regular password changes (every 60–90 days).
   - Introduce Multi-Factor Authentication (MFA) across all critical systems.
3. **Improve Endpoint Protection**
   - Upgrade to enterprise-grade antivirus and Endpoint Detection & Response (EDR) tools.
   - Enable real-time protection and scheduled full-system scans.
4. **Implement Network Segmentation**
   - Separate critical resources (customer databases, backups, project files) from general employee workstations.
   - Limit access based on roles and least privilege.

💾 Backup Strategy Enhancements

- Maintain **offline, immutable, and off-site backups**.
- Ensure backups are performed daily and regularly tested for restoration integrity.
- Avoid storing backups on the same network as production systems.

🛑 Incident Response Process Upgrades

- Develop and formally document an **Incident Response Plan (IRP)** covering:
    - Detection and reporting
    - Immediate containment protocols
    - Communication and escalation processes
    - Recovery procedures and authority roles
- Conduct regular **incident response drills** and tabletop exercises

👥 Employee Awareness & Training

- Schedule quarterly cybersecurity awareness sessions covering:
    - Phishing recognition
    - Safe email and web practices
    - Incident reporting procedures
- Run **phishing simulation exercises** to test employee readiness.

📝 Post-Incident Lessons Applied

- Identify and patch vulnerabilities:
    - Review and update software patches.
    - Disable unused services and ports.
    - Harden workstation and server configurations.
- Monitor systems post-recovery for anomalies and Indicators of Compromise (IoCs).

📊 Business Continuity & Resilience

- Establish a **business continuity plan (BCP)** detailing:
    - Temporary operations workflows during outages
    - Alternative communication channels

- Prioritization of critical services restoration

✅ Summary of Priority Actions:

Action	Priority	Owner	Deadline
Isolate backups from live network	Immediate	IT Manager	Same day
Enforce MFA and strong password policy	Immediate	SysAdmin	1 week
Deploy advanced email filtering	High	IT Security Analyst	2 weeks
Develop formal Incident Response Plan	High	IT Manager	2 weeks
Conduct company-wide phishing training	Medium	HR / Security	1 month

📊 Observations on BrightTech's Current Security Posture

📌 Weaknesses Identified

1. **Inadequate Email Security**
   - No advanced email filtering or attachment scanning.
   - No external email tagging or sandboxing of suspicious attachments.
   - This allowed a phishing email with a malicious PDF attachment to slip through.
2. **Weak Password and Access Controls**
   - Employee passwords were not enforced to be strong or regularly updated.
   - No multi-factor authentication (MFA) in place for sensitive systems.

3. **Poor Backup Management**
   - Backups are performed but stored on the **same network** as live data.
   - This made backups vulnerable to ransomware encryption during the attack.
4. **Basic Endpoint Protection**
   - Basic antivirus software installed, but likely lacking real-time detection and advanced threat prevention.
   - No Endpoint Detection & Response (EDR) solution to detect and contain threats early.
5. **Absence of a Formal Incident Response Plan**
   - Actions taken during the incident (e.g. network disconnection at 8:15 AM) appear ad hoc rather than following a pre-planned, rehearsed protocol.
   - No documented escalation and containment procedures.
6. **Lack of Employee Security Awareness Training**
   - An employee was deceived by a phishing email.
   - No evidence of regular training on identifying phishing attempts or reporting suspicious emails.
7. **No Network Segmentation**
   - Shared drives and customer data accessible across multiple workstations.
   - Allowed rapid spread of ransomware from one machine to others via the shared network

📌 Opportunities for Improvement

Area	Current State	Recommended Improvement

Email Security	Basic filtering	Implement advanced threat protection, sandboxing, and external email labeling
Passwords & Authentication	Weak, rarely updated, no MFA	Enforce complex passwords, regular changes, and roll out MFA for all users
Backups	On same live network	Store backups offline and off-network with regular restoration testing
Endpoint Protection	Basic antivirus	Deploy EDR solutions with real-time behavioral analysis and rapid response
Incident Response Planning	No formal IRP	Develop and rehearse a documented Incident Response Plan
Employee Training	No regular cybersecurity training	Conduct quarterly awareness sessions and phishing simulations
Network Segmentation	Flat network	Segment critical systems and data storage from general user workstations

📌 Overall Assessment

BrightTech’s current security posture is **reactive, fragmented, and vulnerable to basic attack vectors like phishing and ransomware**. To improve resilience, BrightTech needs to **implement layered security controls, formalize response processes, and build a culture of security awareness among its employees**