SBS CyberSecurity

Incident Response Preparedness

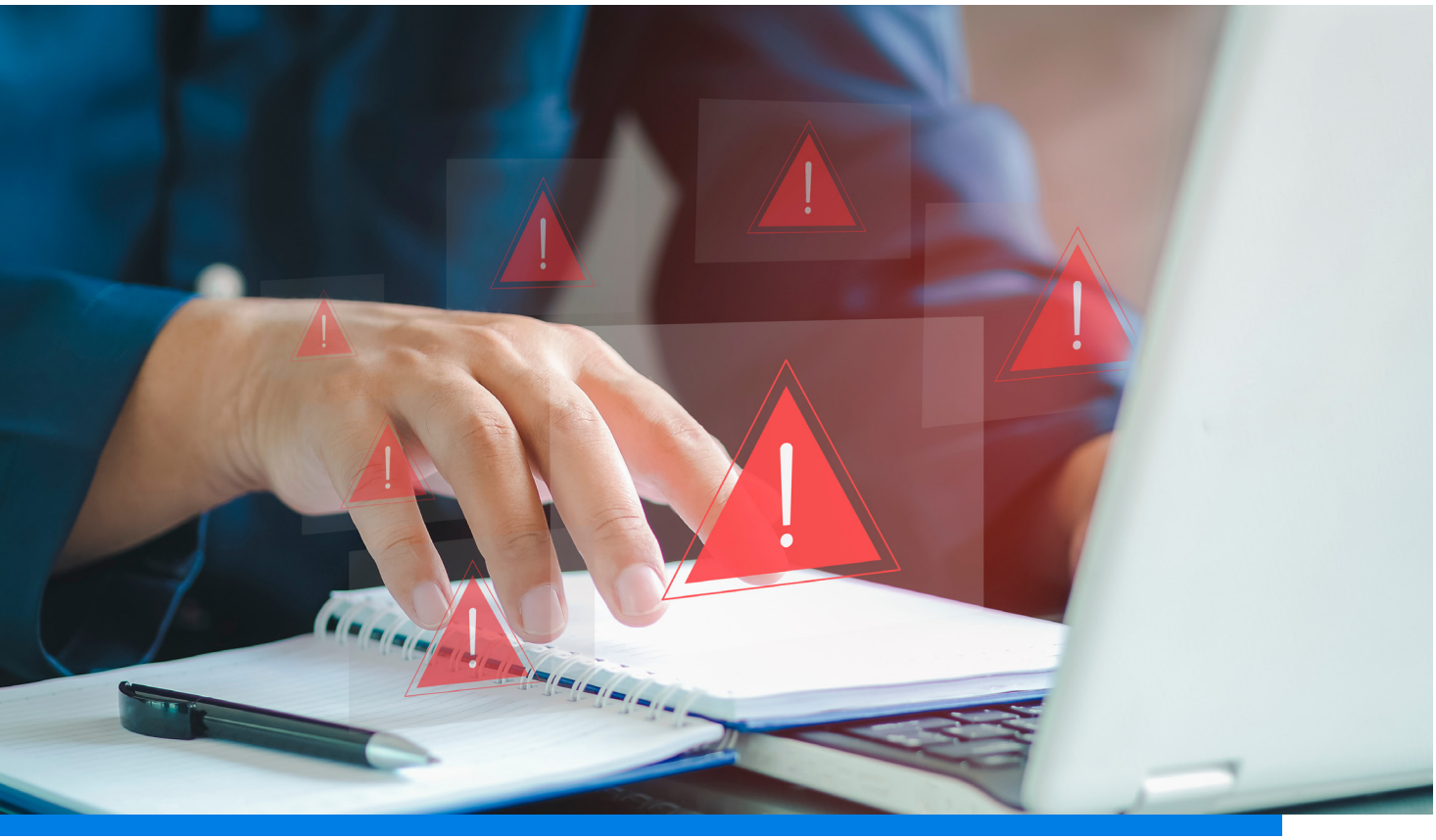
50+ Checklist Items

GETTING STARTED

Imagine waking up to discover your company's network has been breached. Would you be able to tell if someone was in your network? The ability to answer this question can mean the difference between a quick recovery and a costly disaster. Unfortunately, most organizations cannot say 'yes' to this question, which is why many information security professionals are kept awake at night. As an organization, it's crucial to detect and respond to cyber threats quickly. Don't wait until it's too late to take action!

Preparing for an incident means that you have all your ducks in a row in advance so if an incident happens, you can work through the post-incident phases of Incident Response, including detection and analysis; containment, eradication, and recovery; and post-incident items, efficiently and quickly.

If you are uncertain how to prepare for and detect an incident on your network, you are certainly not alone. This checklist will get you started.



PREPARATION

Incident Response aims to mitigate the damage of an attack and/or prevent attacks that threaten an organization's information security. Have the following in place to be fully prepared for an incident:

Risk Assessment

- ☐ Use a comprehensive approach to identify and assess risk pre-incident. Use incident response frameworks to build a comprehensive risk assessment, BCM (Business Continuity Management), and an IRP (Incident Response Plan) that address cybersecurity risk areas (e.g., NIST 800-61, SANS, etc.). Perform and document a gap analysis to identify missing controls related to the framework. Include common potential attack vectors (e.g. Ransomware, phishing, third-party, etc.).

- ☐ To ensure prioritization of recovery efforts, complete risk assessments that include identifying critical assets, potential risks, and controls and prioritize accordingly.

- ☐ Identify the location of critical data and document who has access, manages, or otherwise has control of the data (e.g., IaaS providers, MSPs, etc.).

- ☐ Document all remote access to backups, systems, and organization data, including data shared/hosted with employees, contractors, and third parties.

- ☐ Develop comprehensive data flow diagrams, with data classification of data and systems, and implement the principle of least access to reduce risk to sensitive data.

- ☐ Perform incident response tabletop testing following written IRP procedures and playbooks.

- ☐ When evaluating cyber insurance options, assess the suitability of available cyber insurance policies and consider factors such as coverage limits, premiums, deductibles, and specific risks relevant to your organization.

Response Strategy Planning

Communication Planning

- ☐ Establish efficient communication of the current status of recovery efforts with internal and external stakeholders by creating a detailed communication plan. Include all stakeholders (e.g., Customers, Board of Directors, Employees, Insurance carriers, Regulators, Legal Counsel, etc.).

- ☐ Create prepared notification templates for clients/customers , employees, third-party vendors, federal, state, and local governmental entities or law enforcement, media, regulators, and other stakeholders during an incident.

- [ ] Establish a secure, out-of-band communication channel for the IRT (Incident Response Team) that an attacker or suspect insiders cannot monitor; examples may include cell phones or a secondary encrypted email system. Communicating within regular channels or ticket management systems could tip off bad actors, cause them to move laterally to preserve their access, or deploy ransomware widely before networks or impacted systems are offline.

- [ ] Establish and communicate expectations for the organization's stakeholders. For example, Board of Directors, shareholders, supporters, adversaries, participants, and partners in the value chain. Ensure the IRT understands the expectations for communication and escalation.

Have the following information readily available offline for key organization personnel involved in Incident Response and critical functional areas of your organization:

- [ ] Name
- [ ] Phone Number
- [ ] Email Address
- [ ] Role in the organization
- [ ] Role during an incident

Have the following information readily available offline for vendors that pertain to the management of your network, data, IT assets, or applications:

- [ ] Vendor Name
- [ ] Contact Information
- [ ] Log retention period in months
- [ ] Response time during an incident
- [ ] Who can access the logs

Management Planning

- [ ] Pre-incident policy and procedure must be established, documenting items such as the members and roles of an IR Team, identifying, protecting against, and detecting potential incidents, etc. Identify decision-makers for critical decisions and communications (e.g. Media communication, ransom payments, etc.).

- [ ] Document all controls in place in the BCM/IRP Plan for monitoring organization assets. Include alerting currently in place for DLP solutions, file transfer, malicious or suspicious files, rogue scripts, access, or processes.

- [ ] Establish policies and procedures and document ongoing reviews of preparation items, checklists, and the BCM/IRP plan.

- [ ] Store an offline copy of your most recent Asset Inventory, Network Diagrams, BCM/IRP Plan, and Cyber Insurance Policy in a secondary location for use with communications, strategy, and forensic investigation.

- [ ] Define how incident forms or help-desk tickets are reported upstream – make sure these are encrypted and/or out-of-band communications so potential attackers and insiders can't access or eavesdrop on your ticketing system.

- ☐ Establish how change management needs to occur during an incident, or how you will handle changes to the network and IT assets in an organized manner. Cycling affected devices, emergency changes to systems affecting the uptime of services, critical fix deployment, items that may hamper containment, etc.

- ☐ Establish formal processes and understand legal and regulatory requirements for responding to and reporting breaches in your specific industries, states, and nations. Review preparations with legal counsel.

- ☐ Establish a process for determining and handling criminal activity performed by employees. This only applies to an incident where an employee is the attacker, and it is not an outside threat.

- ☐ Identify and confirm escalation methods and emergency channels with vendors critical to incident response.

- ☐ Ensure response to third-party incidents is included in the organization IRP.

- ☐ Review applicable third-party business continuity management and incident response plans regularly on some defined interval (MSP, MSSP, critical software vendors, etc.). Ensure SLAs align with the organizations MAD, RTO, and RPO.

- ☐ Include forensic investigation, remediation/recovery, or other IR services in MSP/MSSP contracts.

Technology Planning

- ☐ Implement best practices for system hardening aligned with NIST standards, including regular patching and updates, least privilege access controls, changing default system passwords, verifying secure configurations, disabling unnecessary services and ports, and segmenting networks.

- ☐ Deploy advanced technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) solutions, and Artificial Intelligence (AI)/Machine Learning (ML) based threat detection tools to enhance the organization's ability to detect and respond to cybersecurity incidents.

- ☐ Apply the principle of least privilege to all systems and services to limit threat capabilities.

- ☐ Restrict user permissions from installing and running software applications, including limiting local administrator access.

- ☐ Limit the use of remote access to critical systems. Use MFA for all remote and privileged access.

- ☐ Segment networks appropriately to contain the impact of an incident.

- ☐ Implement SPF, DMARC, and DKIM policies for email systems.
- ☐ For Windows, enable Windows Defender Application Control (WDAC), AppLocker, or both on all systems that support these features.
- ☐ Implement Protective Domain Name System (DNS), DNS over TLS (DoT), DNS over HTTPS (DoH), and/or DNSSEC authentication.
- ☐ Consider requiring SMB encryption.
- ☐ Consider implementing zero-trust architecture within the organization's environment.
- ☐ Consider creating service control policies (SCP) for cloud-based resources that limit access to specific services for privileged users.
- ☐ Consider auditing Active Directory (AD) with automated tools that track the actions of users, particularly privileged users and service accounts.
- ☐ Restrict the use of Powershell to specific users for specific purposes on a case-by-case basis.
- ☐ Secure Domain Controllers. Implement a privileged access management (PAM) solution on Domain Controllers to limit access and potential lateral movement or privilege escalation.
- ☐ Regularly patch software and operating systems to the latest available version, prioritizing critical patches.

Evidence Collection Planning

☐ Create a jump bag with the following contents:

- Sanitized drives for drive images
- Incident forms – can be electronic on a laptop or mobile device in the bag
- Printed copy of Incident Response Team (IRT) call tree
- Common hand tools such as screwdrivers or a Leatherman
- Linux live distributions such as Sift, Security Onion, and Kali on bootable DVDs and USB sticks
- Wireshark on a USB Drive (https://www.wireshark.org/download.html)
- Flashlight and extra batteries
- Checklists of all forensic software that might be needed for investigation. Applications like Mandiant Redline and Sleuth Kit should be on this list. Mandiant Redline on a USB Drive (https://www.fireeye.com/services/freeware/redline.html)
- Network tap and LAN cables, or the capability to create span ports on your switches.

- ☐ Determine where digital forensic data will be stored/maintained for chain of custody integrity, preferably in an out-of-band location. Notify all stakeholders managing evidence of the location.

- ☐ Ensure third parties understand the requirements for preserving evidence within their control.

Restoration Strategy Planning

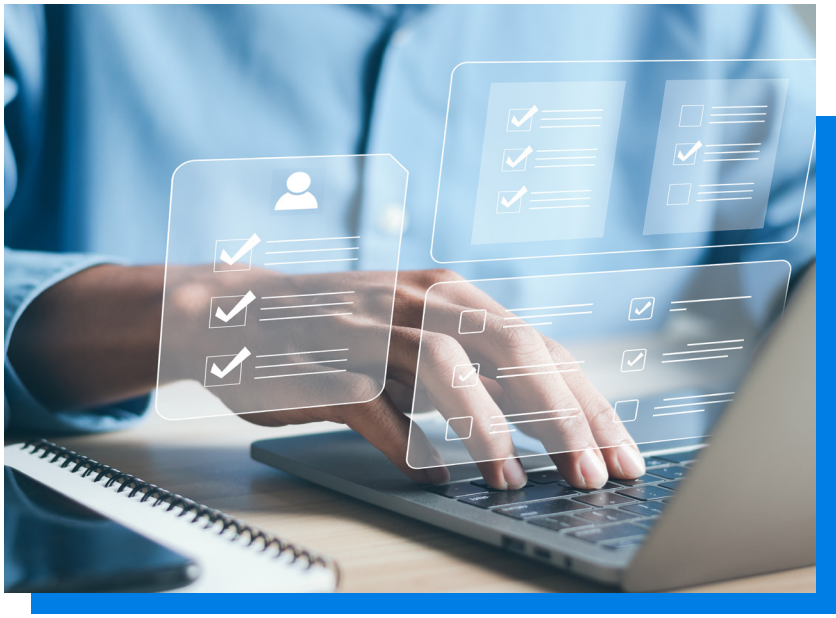
- ☐ Develop a post-incident restoration strategy in the BCM/IRP.

- ☐ Ensure controls have been implemented for backing up critical systems and data.

- ☐ Document current controls/procedures in the BCM/IRP that prevent backups from being affected by common potential attack vectors (e.g., Ransomware, adopted unauthorized access, lateral movement, MFA bypass, network segmentation, etc.).

- ☐ Maintain offline, encrypted backups of critical data. Ensure at least one backup of critical data or systems is air-gapped or immutable.

- ☐ Retain backup hardware to rebuild systems if the primary system is not recoverable.



Training and Testing

- ☐ Budget to conduct continuous training. Include annual security awareness training that includes common potential attack vectors (e.g. Ransomware, phishing, social engineering, etc.) as part of employee onboarding and ongoing organization-wide training programs.

- ☐ Require targeted, role-specific first responder training for help desk or customer-service employees, including what to look for and how to "push the red button" and report potential incidents. Frontline staff are your human sensors. Triage should be tested and trained.

- ☐ Establish regular IRP testing – work through common IR scenarios and incident types by creating incident response playbooks for common, current threats (e.g. Ransomware, BEC, network intrusion, etc.). Identify areas of improvement, especially communication and command structure. Include relevant third parties in IR testing.

- ☐ Review third-party service level agreements, vendor agreements, BCM/IR plans, and incident command structure. Participate in third-party IRP testing and response where applicable.

- ☐ Ensure all stakeholders understand their roles and responsibilities in the event of an incident. Practice standing up a command center, relevant workstreams, and reporting structure.
- ☐ Periodically conduct IR drills – use network testing (Penetration Testing) separate from the IRT if possible.
- ☐ Conduct a simulated ransomware attack to assess the organization's incident response capabilities, identify potential vulnerabilities, and validate the effectiveness of protective measures.

DETECTION & ANALYSIS

How do you detect an incident once your organization is prepared? The answer isn't simple to explain, but detection can be simple for IT personnel or third-party MSSP's who understand what "normal" looks like on the network. The detection capability comes from watching the logs specified below and looking for anomalies or separations from the baselines of your network. To accomplish this, the following should be in place.

IT Operations

- ☐ Network Time Protocol (NTP) must be turned on and configured for all devices sending logs.
- ☐ Establish a "one user, one account" rule for accountability reasons; sharing of accounts should never be allowed!
- ☐ Establish secondary accounts for privileged access and changes, for accountability reasons.
- ☐ Never use a domain admin or privileged account to answer emails or browse the Internet.

- ☐ Ensure service accounts are assigned to only the services they run.

Logging

- ☐ Ensure logging is enabled for all critical systems.
- ☐ If a SIEM or SOAR solution is in place, ensure the solution successfully consumes all potentially useful log files.
- ☐ Define proper SIEM/SOAR and/or MSSP security alert thresholds.

Verify the ability to perform log analysis in the following areas:

- ☐ SIEM Logs
- ☐ Firewall Logs - Both ingress and egress logs are necessary for proper log correlation in an incident.
- ☐ Internet Service Provider (ISP) Traffic Logs
- ☐ IDS/IPS Logs
- ☐ DNS Logs
- ☐ Network switch ACL logs
- ☐ Advanced Malware Protection Logs (e.g. EDR, MDR, XEDR, etc.)
- ☐ Windows Event Logs
- ☐ Active Directory (AD) Logs
- ☐ Unix/Linux Logs
- ☐ Cloud
- ☐ VPN/Remote Access, Monitoring, and Management Logs (RMM)
- ☐ Web Proxy Logs
- ☐ Content Filtering Logs (e.g. Website, Email, etc.)
- ☐ Data Loss Prevention (DLP) logs
- ☐ Mail Server Logs
- ☐ SQL and Database Logs

At a minimum, monitor these key areas:

- ☐ Total Network Logs per Second
- ☐ Patch Management %/Known
- ☐ Vulnerabilities
- ☐ Denied FTP/SFTP Requests
- ☐ Denied Telnet/SSH Requests
- ☐ Failed Remote Logins
- ☐ VPN Connections/Failed VPN Connections
- ☐ Blacklisted IP blocked
- ☐ Location connectivity lost
- ☐ New privileged credentials created
- ☐ Threshold for successive account lockouts
- ☐ VLAN ACL violations
- ☐ Changes to Group Policy
- ☐ Increase in network bandwidth
- ☐ Increase in outbound email traffic
- ☐ DNS Request anomalies

CONTAINMENT, ERADICATION, & DISCOVERY

This is a critical step in the IR process that must be entered into cautiously following the guidance in the IRP. If drastic measures are taken without considering the consequences, critical forensic information may be lost, and cyber insurance may refuse to pay a claim.

Containment Strategy

Risk Management

- ☐ Contact your cyber insurance provider to report the incident.
- ☐ Ensure all required notifications are completed to all governmental, regulatory, law enforcement, or other entities within the required time frames.
- ☐ Prioritize immediate concerns.
- ☐ Assess in real time the risk of acting or NOT acting. This is critical to avoiding mistakes.
- ☐ Ensure incident response team members document all actions taken. Track all privileged access actions, if possible.

Real-Time Evidence Collection

- ☐ Establish a secure evidence collection process and ensure evidence integrity. Prevent attackers or insiders from accessing secure areas.
- ☐ Establish "contain and clean" criteria based on desired evidence preservation for each incident type and immediately isolate impacted systems, if possible.
- ☐ Establish "Watch and Learn" or "Pull the Plug" criteria. "Watch and Learn" means you will watch the attacker work through the attack briefly before pulling the plug to gather evidence. "Pull the Plug" means you will eradicate the threat before gathering evidence. If pulling the plug is decided, power down devices if they cannot be unplugged to minimize the attack's spread.
- ☐ Examine all available logs and alerts for indicators of compromise, particularly logs before the event's detection and before any restoration from backups. Restoration from a backup can restore backdoor access for an attacker if created before detection.
- ☐ Take a system image and memory capture of affected devices (e.g., workstations, servers, virtual servers, and cloud servers).
- ☐ For cloud resources, take a snapshot of volumes to get a point-in-time copy for reviewing later for forensic investigation.

- ☐ Preserve and secure any communications from attackers (e.g. ransom notes, emails, etc.).
- ☐ Research trusted sources for mitigation and containment techniques and guidance for the incident type (e.g. FS-ISAC, MS-ISAC, CISA, NSA, FBI, security vendors, etc.). Consult federal law enforcement agencies if decryption services are needed.
- ☐ Complete a technical threat assessment. Determine if sensitive information has been compromised or exfiltrated.
- ☐ Identify all affected systems based on the critical asset list for triage. Ensure monitoring of unaffected systems so they can be deprioritized.
- ☐ Initiate threat-hunting activities, if appropriate.

  - Recent account creation or credential dumps.
  - Recent system modifications, new services, child services, or scheduled tasks.
  - Anomalous remote access usage, login activity, or Powershell use.
  - Signs of recent file updates, file renaming, or file upload/downloads.
  - Run packet capture software, if appropriate.

- ☐ Contain associated authentication systems that may be used for continuous access (e.g., VPNs, SSO, cloud, or public-facing assets.) Examine systems for outside-in and inside-out persistence.
- ☐ Evaluate backups and restore solutions for possible recovery use or for loss due to backup compromise. Prioritize restoration, recovery, and system rebuilding activities based on the critical asset list.

RECOVERY & POST INCIDENT ACTIVITY

Restoration and Recovery Strategy

- ☐ Identify all systems and accounts involved in the initial incident, including email accounts. Issue password resets for all affected accounts and systems.
- ☐ Ensure all evidence has been collected from internal and third-party stakeholders and properly secured for chain of custody.

- ☐ Restore and reconnect systems from offline, encrypted, immutable backups. Ensure clean systems are not reinfected.
- ☐ Identify any data lost during the incident and initiate notifications as required by law or regulation.
- ☐ An appropriate organization authority should declare the incident over based on established IRP criteria and notify stakeholders accordingly.
- ☐ Document the incident with all pertinent information including:
  - Scope of the incident
  - Type of sensitive information impacted, if any.
  - Information systems and any third parties involved.
  - Incident action or steps all stakeholders take to identify, analyze, contain, and recover systems and data.
  - Resolution summary and notification actions.
- ☐ Conduct after-action reviews, identify lessons learned, and update training, the BCM/IRP plans, policies, or procedures accordingly

Free Resources

available at: sbscyber.com

Hacker Hour Webinar

Join our free monthly interactive webinar series focused on discussing cybersecurity issues and trends.

Product Demos

Discover the power of our offerings with live demos scheduled each week highlighting individual products and services.

Security Awareness Training

Share our cybersecurity training tools with both your employees and your customers.

TRAC™ Action Tracking

Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

Join Our Email List

Follow the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity.

Your Cybersecurity Ally

SBS CyberSecurity, LLC (SBS) is a top-rated consulting and audit firm. With over 20 years in the cybersecurity industry, SBS has provided solutions to thousands of regulated organizations across the United States and abroad. We offer dynamic solutions to help you build a proactive risk management program capable of withstanding the daily threats your organization faces. Our services are designed to assist you in making informed cybersecurity decisions to better protect your business.

For more information:
sbscyber.com | 605.923.8722

SBS CyberSecurity