

50+

Incident Response Preparedness Checklist Items



www.sbscopyber.com

Written by: Buzz Hillestad, Senior Information Security Consultant at SBS CyberSecurity, LLC
and Blake Coe, Vice President, Network Security at SBS CyberSecurity, LLC



GETTING STARTED



The #1 question organizations need to ask themselves is “if someone was in our network, would we be able to tell?” An organization’s ability to answer that single, extremely important question makes all the difference between being able to respond and recover from an incident quickly (and cost-effectively) vs. being notified by a user, or worse yet, by a federal agency, that something is amiss. Be honest with your answer; most organizations are unable to say “yes” to this question, and it rightfully keeps many networking admins or information security professions awake at night.

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. You will need the following items prepared ahead of time:

- Configurations
- Logging
- Vendor Information
- Key Personnel
- Detection Monitoring

If you are uncertain how to go about preparing for and detecting an incident on your network, you are certainly not alone, this checklist will get you started.

CONFIGURATIONS

Have the following items configured and in place to be fully prepared for an incident:



- Network Time Protocol (NTP) must be turned on and configured for all devices that will be sending logs.
- 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.
- Establish a central logging capability (syslog, syslog-ng, snare, etc.)
- 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 uptime of services, critical fix deployment, items that may hamper containment, etc.
- 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 email or browse the Internet.
- Ensure service accounts are assigned only to the services they run.
- Store an offline copy of your most recent Asset Inventory to be used for forensic investigations
- 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
 - Mandiant Redline on a USB Drive (<https://www.fireeye.com/services/freeware/redline.html>)
 - Wireshark on a USB Drive (<https://www.wireshark.org/download.html>)
 - Flash light 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
- Network tap and LAN cables, or the capability to create span ports on your switches.
- A secure communication channel for the IRT that cannot be monitored by an attacker or inside; examples may include cell phones or secondary encrypted email system.

CONFIGURATIONS, continued

- First responder training for help desk or customer-service employees, including knowing what to look for and how to “push the red button” for potential incidents. Frontline staff are your human sensors.
- Define how incident forms or help-desk tickets are reported upstream – make sure these are encrypted so potential attackers and insiders can’t access or eavesdrop on your ticketing system.
- Establish regular Incident Response testing – work through common IR scenarios and identify areas of improvement, especially communication and command structure. Budget to conduct continual training. Triage should be tested and trained. Service level agreements, vendor agreements, and incident command should be worked through and tested. Periodically conduct IR drills – use network testing (Penetration Testing) separate from the IRT if possible.
- Establish a secure evidence room with locking cabinets to facilitate secure collection of evidence and ensure no modification by attackers or insiders.
- Establish “Watch and Learn” or “Pull the Plug” criteria. “Watch and Learn” means you will watch the attacker work through the attack for a bit before pulling the plug on them as a means of gathering evidence. “Pull the Plug” means you will eradicate the threat before gathering evidence.
- Establish “contain and clean” criteria based on desired evidence preservation for each incident type.
- Establish and understand legal and regulatory requirements for responding to and reporting on breaches in your specific industries, states, and nations.
- Establish a process for determining and handling criminal activity performed by employees. This item only applies to an incident where an employee is the attacker and it is not an outside threat.
- Establish organization’s stakeholder expectations. For example, Board of Directors, shareholders, supporters, adversaries, participants, and partners in the value chain. Ensure the IRT understands these expectations.
- Establish criteria for continual review of preparation items in this list.

LOGGING

At a minimum, turn logging on in the following areas:

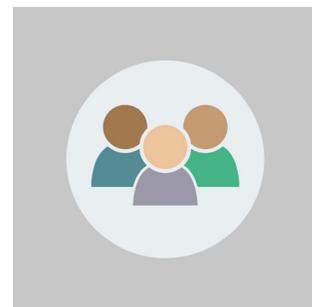
- Firewall Logs - both ingress and egress logs are necessary for proper log correlation in an incident
- Internet Service Provider (ISP) Traffic Logs
- IDS / IPS Logs
- AV Logs
- Web Proxy Logs
- Content Filtering Logs
- Windows Event Logs
- Active Directory (AD) Logs
- Unix / Linux Logs
- VPN / Remote Access Logs
- DNS Logs
- SIEM Logs
- Data Loss Prevention (DLP) logs
- Mail Server Logs
- SQL and Database Logs
- Switch ACL logs



VENDOR INFORMATION

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

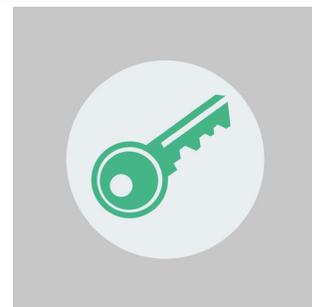
- Vendor Name
- Contact Information
- Log retention period in months
- Response time during incident
- Who can access the logs



KEY PERSONNEL

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

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





DETECTION MONITORING

Now that your organization is prepared for an incident, how do you detect one? The answer isn't simple to explain, but detection can be simple for IT folks that understand "what normal looks like" on their network. The detection capability comes from watching the logs specified above and looking for anomalies or separations from the baselines of your network.



At a minimum, watch logs in these key areas:

- Total Network Logs per Second
- Patch Management % / Known Vulnerabilities
- Denied FTP Requests
- Denied Telnet Requests
- Failed Remote Logins
- VPN Connections / Failed VPN Connections
- Blacklisted IP Blocked
- Branch Connectivity Lost
- New Admin 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

ADDITIONAL FREE RESOURCES

available at www.sbscyber.com.



MONTHLY HACKER HOUR

Join our 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 or services.



SECURITY AWARENESS TRAINING

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



CYBER-RISK™

Go beyond the spreadsheet with an automated FFIEC cybersecurity assessment.



TRAC™ ACTION TRACKING

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



JOIN OUR MAILING LIST

Stay current with the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity. Join our email list and be in the know!

ABOUT US

YOUR CYBERSECURITY PARTNER

SBS CyberSecurity, LLC (SBS) is a premier cybersecurity consulting and audit firm. Since 2004, SBS has been dedicated to assisting organizations with the implementation of valuable risk management programs and to mitigating cybersecurity risks. The company has provided cybersecurity solutions to organizations across the United States and abroad. SBS delivers unique, turnkey solutions tailored to each client's needs, including risk management solutions, auditing, and education. SBS CyberSecurity empowers customers to make more informed security decisions and trust the safety of their data.

FOR MORE INFORMATION PLEASE VISIT WWW.SBSCYBER.COM OR CALL 605-923-8722.

