SkyViewTek

Incident Response Preparedness CHECKLIST

In an evolving cyber threat environment, businesses of all sizes and complexity operate with some degree of attack risk. Having a plan of record and related policies for worse-case incident response is foundational to good security preparedness. However, many organizations find the process of pulling together all the many considerations and factors confusing and frustrating.

As a company dedicated to providing our clients with proven cybersecurity services, we share the following considerations as developed by NIST (National Institute of Standards and Technologies). As a long-standing leader in cybersecurity standards, guidelines, and best practices to meet the needs of U.S. industry, federal agencies, and the broader public, NIST's Computer Security Incident Handling Guide is an excellent resource to help inform your discussion and planning considerations for incident response.

Here's a summary checklist for review against your current incident response preparedness.

INCIDENT RESPONSE PREPAREDNESS

☐ **Establish a formal incident response capability.**
Be prepared to respond quickly and effectively when computer security defenses are breached.

☐ **Create an incident response policy.**
Your incident response (IR) policy is the foundation of an IR program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items.

☐ **Develop a plan based on the incident response policy.**
Your IR plan provides a road map for implementing an IR program based on your defined policy. The plan indicates both short and long-term goals, including metrics for measuring the program. The IR plan should also indicate how often incident handlers should be trained and the requirements for incident handlers.

☐ **Develop incident response procedures.**
IR procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the IR process. The procedures should be based on the IR policy and plan.

☐ **Establish policies and procedures regarding incident-related information sharing.**
You should communicate appropriate incident details with outside parties, such as the media, law enforcement agencies, and incident reporting organizations. The IR team should discuss this with your appropriate business management leadership and legal counsel to establish policies and procedures regarding information sharing.

☐ **Provide pertinent information on incidents to the appropriate organization.**
Federal civilian agencies are required to report incidents to US-CERT; other organizations can contact US-CERT and/or their ISAC. Reporting is beneficial because US-CERT and the ISACs use the reported data to provide information to the reporting parties regarding new threats and incident trends.

☐ **Consider the relevant factors when selecting an incident response team model.**
You should carefully weigh the advantages and disadvantages of each possible team structure and staffing model in the context of your needs and available resources.

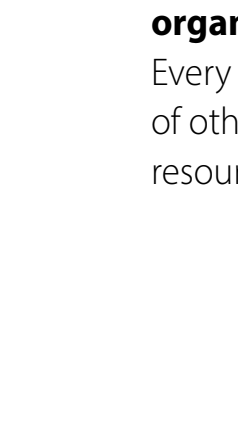
☐ **Select people with appropriate skills for the incident response team.**
The credibility and proficiency of your team will largely depend on the technical skills and critical thinking abilities of its members. Technical skills include system and network administration, programming, technical support, and intrusion detection. Teamwork and communications skills are also needed for effective incident handling. Necessary training should be provided to all team members.

☐ **Identify other groups within your organization that may need to participate.**
Every IR team relies on the expertise, judgment, and abilities of other teams, including management, legal, and human resources to name a few.

☐ **Determine which services the team should offer.**
Although the main focus of the team is incident response, additional functions may include monitoring intrusion detection sensors, distributing security advisories, and educating users on security.

GOOD DEFENSE WITH A TRUSTED SECURITY PARTNER:

For many organizations, staffing and budget resource constraints prevent implementation of best practice incident response measures. A trusted security partner can fill many gaps in this critical element of good defense in-depth.



To learn more about the recommendations provided and how managed cybersecurity solutions can deliver on important 24/7 monitoring and response, please give us a call.

SkyViewTek
5 Great Valley Parkway - Suite 210, Malvern, PA 19355,
Malvern, PA 19355
6105905006