The Phases In The Incident Response Plan

Coming by a strange occurrence in the field of Information and Technology is always a moment of worry as it is an indication of something bad that’s about to happen. The HIPAA Security Standards define an incident as “The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

This would seem to be a rather broad terminology used in the terms of IT, but in general, it could be said to be something like a breach of the security system for various reasons. Now when a breach occurs in a security system, you must be available with a full-fledge robust plan as the following.

Preparation Is Most Important

Preparation for the worst is always the most successful strategy in carrying out organized operations and tasks of the day, and the incident response plan stands no different.

The preparation in advance for a set of protocols and procedures to follow in case of the occurrence of an incident is always the most important thing to do. Have a set of procedures and protocols that are practiced by your employees and the management is your best shot at ensuring that when an actual incident happens, the recovery and remediation will be swift and the quickest.

Now when you react quickly and take less time to recover, you would have potentially saved yourself from bigger damages before they could even occur.

Identify The Nature Of The Incident

Now once that you have an incident and crisis at hand, you will never have a good shot at recovery if you do not know the nature and threat level of the problem. The first and foremost thing to do when an incident occurs is looking for the cause of it.

The identification is important and it can be done by consulting a series of question regarding:

- The type of incident that has occurred.
- Is it an attempt towards data theft from the system?
- Is the threat an external one or is it the one from the inside?
- Whether or not it is a network threat?

These are all examples of the type of questions that needs answering when you are identifying the type of threat. Once the threat has been identified, you can then switch to procedures and protocols that your company has prepared (as mentioned above) and tackle the problem before bigger concerns arise and more damage is done.

Containment Of The Threat

After the identification phase, your best policy should be dealing with the incident in a manner as quick as you can. The quicker you are at acting to contain the problem, the better chance you would have against data theft or any security breach.

The notification of the right people is of the utmost importance. When the right people in your organization are notified on time, you can always arrive at the best possible solution for the containment of the threat in time, whether it would mean the isolation of the area that has been infected or not, all is left to the experts to decide.

This is also the phase where you properly equip yourself with the right tools and ensure you have all the brains needed to contain the incident.

Remediation Of The Breach

By now you should be in decent control over the situation as you have settled all the information regarding the incident and stopped it from spreading and growing even more. The next step would be to proceed towards the termination and expulsion of the threat.

Remediation is the resolving of the identified issue at hand that can be:

- The removal of malicious code if there is any.
- The termination of the threat.
- Even the removal and termination of any employees or personnel onboard that are linked to the happening of the incident.

You also need to decide at this point whether or not the backups will need to be implemented and the nature of the security weakness that should be immediately addressed.

Time To Recover

If you find yourself at this point in the incident response plan, you have dealt with all the threats and the breach that had happened to your security system. Now you need to focus all your energies back on getting your system up and running again.

Although the threat has been dealt with, you need to closely monitor the activities for a designated time even now to make sure that all of the threat has been dealt with and that no anomalies remain now. Monitoring should aid you in detecting any suspicious activity if there is any happening at all. This is ensuring the fact that all of the policies and procedures of your company are up and running in a well-monitored condition.

Lessons Learned For The Future

Even though you have dealt with all the threats and breaches that had happened to your system, it may not be the time celebrate and get going with the affairs of the day just yet. There is a dire need for compiling a detailed report right now that should cover the complete peculiarities of the information and the incident.

This report should include:

- The possibilities because of which the breach or the incident took place.
- What could possibly have been an ideal precautionary measure that could have prevented it in the first place?
- Whether or not your security system requires an update to make sure nothing of the sort will happen again?
- And also the intended person to whom the information should be processed and forwarded.

The preparation for the worst-case scenarios when it comes to the protection of your business is equal in importance to prevention. Incidents and breaches are going to happen no matter how immaculate you think your designs are, but it should always be taken as something to learn from rather than regretting that it happened. Having a robust Incident Response Training of your employees and management could possibly save you fortunes and peace of mind.