What outside entities should be considered when handling security incidents?

Arielle McGlone

October 6, 2019

When handling a security risk, other things that you should think of when you're being targeted is that the attacker might be a criminal, he might just want money from you. If they do want money from you it's not a good idea to just give it to them, you should refer to outside help, so you can better assess the problem. You should think about your employees and the information that your company possess, because they might use that to threaten you. Also, if you probably resist they might expose sensitive information about you to the whole company. Also take in the fact that you might need to respond quickly and if you take too long that could cause more damage. Your response team depends on the size of your organization, so it could be a central incident response team, distributed IRT or coordinating team. The type of team should be considered meaning if you want the Incident response team to have 24/7 availability, to be Full or Part-Time members or employee morale. This also plays in with factoring the cost and the type of expertise that you need for the job. The heavier the job is you will have to pay more, and you will need to look for outside help when trying to fix the problem. Also, you have to pick the right outside agency to help and make sure they fit your specifications and qualifications. It is also important that you also contact a law enforcement agency as soon as the problem arises. The most important is communicating with your team that you are being attack but the key is knowing how to talk to them. You want to make sure that you have a training session on talking to the media if it comes to that, so they can say the right thing to them. Also, when talking to the employers notify them that whatever they can contribute to the investigation it is vital. All the departments play an important role in handling the incident which the incident response team should realize. Other things that you should do is have an incident response policy which will help you develop a response plan which provides detailed steps on handling the situation. You should also discuss information sharing policy and procedures with employees when dealing with outside agencies and the media. In that plan there should be motives made to prevent events such as this from happening again, and having risk assessments and making sure you secure your hosts and networks the best way possible should be a thing that you should practice. These are only some of the outside entities that should come into factor when dealing with a security issue. I think that as long as you have a plan to follow for handling an incident and the owner communicates with its incident response team closely until it's handled, and you keep the employees as up to date as possible it will most likely not affect them or your company as much, and you can help things run as smoothly as possible while going through a crisis like this.

Reference:

NIST. (n.d.). Computer Security Incident Handling Guide, *Revision 2*(800-61), 1–51. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf