My Business Network Has Been Hacked, What Next?

You've just been informed you that your company networks have been hacked.

Now, if you took the time to set up an incident response plan, you're good! You can follow that through, and ignore this article. If not, here are four steps to get you through.

Step One. Call in the right people.

This is going to be a changing cast of people, depending on the situation.

If proprietary information has been accessed -- the core of what gives your company value -- you need to call the board of executives. If corporate network has been breached, and the FBI were the ones to tell you, you need to get hold of the company legal officer.

Work together with the people involved to gain knowledge of what's happened, how much damage has been done, and what legal action needs to be taken.

Step Two. Make a plan.

Take the knowledge you gained in the last step, and extrapolate it into a plan of action. This is different from the incident response plan we mentioned in the beginning, and is instead specific to this instance. It should lay out the particular steps that need to be taken to handle the damage. It should include communication: what to tell the board, law enforcement, employees and the public.

The plan must include the technical analysis of the breach, and who is going to participate, as well as what their roles will be. The plan needs to include the steps for finding out where the active threat still is, and how to partition it off from the rest of the network until it's successfully cleaned up.

Step Three. Lead the team.

As the team lead, your job is clearing any road blocks that keep the team from doing their jobs. Since most team members have responsibilities other than incident response, you need to be clear with their managers that this is a priority.

Step Four. Call in experts to buff up your security.

You've discovered what happened, and you've taken the steps to resolve the legal sides of the problem. What do you do to fix the security side, though? If your own team is unable to find a fix, consider in calling outside experts. Working with a team like Combined Systems Technology can help your own people learn new skills, as well as build up your security to prevent further attacks.

If you're interested in learning more about how we can help you get ahead of this worse case scenario, please contact us.

CST
Combined Systems Technology
800-944-2966 515-270-5300
www.cstoncall.com info@cstoncall.com