Cyber Breaches And Incident Reporting

Back in 2016, Uber suffered a breach that cost it about $100,000. Sounds terrible, right? But it can get so much worse.

Uber failed to properly report the incident and take the measures it needed to take. A few years later, those actions resulted in a fine of $148 million. Certainly, that's way worse than what the hackers initially stole.

There are a few lessons to take from this:

• What you do in your response phase after a breach or incident is just as important, and possibly even more impactful, than what you do in your protection phase.

• You need to act on a breach or incident as soon as you think you have one.

• You need to encourage your employees to do the same.\

Some organizations attempt to deliver this message to their employees through fear by telling them things like, “If you click on the wrong link and we get breached, you’ll get in trouble.” All that is going to do is cause them to hide what they may think is a breach or incident. You need to understand that cyber breaches happen every day, and what you do next can make things so much worse.

Empowering your employees to do the right thing helps them become part of the solution instead of part of the problem.

To make it easy on you to have this conversation with your employees, here are six considerations you can share with your team that will help them determine whether a cybersecurity incident has taken place.

• Was the confidentiality, integrity or availability of data, information systems or computer assets belonging to you or your organization potentially exposed?

• Was IT equipment lost or stolen?

• Were explicit or implied security policies violated?

• Were network or computer systems breached or attacked?

• Was there inappropriate use or unauthorized access?

• Did another person display suspicious behavior?

Once it's determined that a security incident happened, employees should be encouraged to immediately report on the following:

• Is the incident still in progress?

• What are the details pertaining to the incident?

• When did the incident occur? (Include both the date and time.) If you're not sure, then when did you first become aware of the incident?

• Where did it occur? (This could be a physical location or a digital one, such as in a directory on your computer.)

• Who caused the incident?

• How did you discover the incident?

• Did you do anything in response?

Who they should report this information to will depend on the incident and on your organization. In some cases, the incident may be reported to IT, HR or accounting. There have even been cases where the incident was reported to the legal team. When in doubt, it is best to get employees to review your corporate security policy or ask their direct supervisor for guidance. If you don't have a corporate policy, or you have one but this isn't addressed in it, then now is the perfect time to start.

When you're faced with the dilemma of whether or not to report a security incident, just remember the story with Uber.

Uber may have thought that it would be better to avoid the trouble and embarrassment of its $100,000 cybersecurity breach. But by not reporting the incident, Uber made its $100,000 problem more than one thousand times worse because it was fined $148 million for failing to properly report that cybercrime.

You are not doing yourself or your friends any favors by not reporting a security incident. Instead, like Uber, you risk making things over one thousand times worse.