SpencerFane®

# Ransomware: Plan for Disaster

As you get to work in the morning, you find your keycard will not let you into the office. You try a different entrance. That door also does not open. You call the company's IT department to see what is going on to find out that the company's phones only ring to a dial tone. The phones are down.

You see someone else arrive and try their keycard; it also doesn't work. Between the two of you, you try every coworker's cell phone number you know to let you into the building. No one is inside; everyone is still on their way in. You finally get ahold of someone who works from home and find out the computer has a message displayed on the home screen.

**Your files are encrypted.**

Panic is now setting in and questions race through your mind:

- Now what?
- Who should be told?
- Do we tell anyone?
- How do we fix this?
- Can we fix this?
- Is this why the phones and keycards do not work?
- What about my stuff locked in the building?
- Do we have insurance for this?
- How did this happen?

If you have been watching the news lately, you know the above scenario can happen to you and your company. At the time of writing, the largest and most recent was the ransomware attack on the Port of Nagoya in Japan. Hopefully, you will have a plan in place before you reach this stage.

**What should I do to prepare for an attack?**

The first thing to do is create a team of people who will be there to assist and cover different roles in getting the company back on its feet.

**Isn't this all just IT's job?**

No. Managing a hack or ransomware attack is not a simple matter. You need people in place from all across the spectrum to get things back online. While it is true IT will help with both preventing and remediating an attack, there are also duties that must be taken care of while you get back up and running.

**What else is there to do besides fixing the computers?**

There are multiple moving parts that need to be handled while trying to repair your systems. While there are multiple things that need to be covered, some important ones to consider are:

1. Communications
2. Accounting
3. HR
4. IT and Cybersecurity (internal and external)
5. Security Operations Center (SOC)
6. C-levels (COO, CEO, CIO, etc.)
7. Counsel

The above are just a sampling of who should be in the group to help should a hack occur. There are other types of professionals that should be on the list, but the above should get you and your company started.

**Just make a team and that's it?**

No. It is great to have a team, but every team member should know every other team member. You also need to have backups for each person. What happens if your communication team member is on vacation or ill when an attack occurs? You should be prepared for such an eventuality.

**Is that all?**

No. Just because the team is created and the members know each other (and you have a backup for each member) does not mean that the company is ready to handle an attack. The team should practice how to respond to an attack.

**What next?**

Finally, if you have cyber insurance you should review your policy. Many insurers require pre-approval of third party vendors before an attack occurs. If you know who you want to use, you should contact your insurer and make sure your preferred third party is on the insurer's approved list.

*This client alert was drafted by David Brininger and Shelby Menard, attorneys in the Spencer Fane Houston and Plano, Texas offices, respectively. For more information about this issue, please visit www.spencerfane.com.*