Dos and Don'ts
for Responding to a Ransomware Incident

Do you know what to do when you have discovered a ransomware incident? Time is of the essence, but it is also critical to take appropriate action to secure the network, contain the incident, and preserve the evidence. Here are a list of the immediate next steps to take after discovering a ransomware attack:

✗ **DON'T** wipe everything and start over. Wiping everything and starting over from backups destroys critical forensic evidence about how the incident occurred and what the threat actor did during the incident.

✔ **DO** make at least one copy (preferably two copies) of all systems before beginning restoration and recovery efforts. Making a copy preserves evidence for the forensic investigation.

✔ **DO** check to see if you have cyber insurance and contact your insurance carrier immediately.

✔ **DO** check your contracts with clients and/or vendors for any potential data breach notification clauses. Contracts can define a breach differently, and can have a much shorter turnaround time for notifications.

✗ **DON'T** initiate communications or otherwise engage with the threat actor. Leave that to the professionals!

✗ **DON'T** file any regulatory reports before engaging counsel. Even though you may be the victim of a ransomware attack, you don't actually if there has been a breach as defined in the applicable laws. Engage counsel and discuss any concerns before filing anything.

✗ **DON'T** say the B word (breach)! You can communicate regarding the incident to employees, clients, or customers. But you don't know that there has been a breach yet. You have discovered a network outage, or an incident impacting your network.

✔ **DO** activate your Incident Response Plan.

✔ **DO** engage counsel ASAP to help identify the resources necessary to contain, restore, and investigate the incident. Counsel can also assist.

For assistance with any data security incident contact the Lewis Brisbois Data Privacy and Cybersecurity team at 888.427.8855 or BreachResponse@lewisbrisbois.com.