troutman sanders

Ransomware Attacks Amid COVID-19

There is never an opportune time to be the victim of a ransomware attack, but with the growing impact that COVID-19 is having on businesses and the increased pressure they already face, a ransomware attack in today's environment could certainly prove to be disastrous. Cybercriminals are leveraging the pandemic for their commercial gain and we have already seen several businesses fall victim to these types of attacks, including businesses in the health care and legal industry.

If your business finds itself in a similar position, or if you are among the smarter businesses who are planning ahead, below are the questions to consider:

PREPARATION

- Do you have a plan in place to respond specifically to ransomware attacks and have personnel been trained on response procedures including through tabletop exercises?
- Do you have cyber insurance that would cover you in the event of a loss?
- Have you pre-selected experienced outside counsel to assist with navigating the response?

TO PAY OR NOT TO PAY?

- Are there backup systems in place to replace compromised systems?
- How long can your organization withstand systems being down?
- Have you considered the business repercussion of not paying?

PAYING THE RANSOM

- If you decide to pay, does your organization know how to obtain cryptocurrency?
- Do you know who to call to assist with ransom negotiations?
- Have you considered the possibility that even after paying, recovery may be limited?

SECURITY

- Are current systems segregated to minimize damage in the event of this type of attack?
- Have you disconnected impacted devices from all network connections?
- Have you preserved/secured access logs to determine when systems and networks were accessed, what was uploaded, etc.?
- Have you investigated to determine whether attackers have left any backdoors on the system to allow for reentry?

RECOVERY

- Do you have Business Continuity Plans or Disaster Recovery Plans in place?
- If recovery or backup systems are available, have you confirmed that those backups have not also been compromised, or are susceptible of being compromised, prior to going live?
- If no backups are in place, can systems be rebuilt, or data be recovered, with minimal loss?

LEGAL ISSUES

- Have you considered whether payment to attackers violate U.S. laws or government sanctions (e.g., the OFAC list)?
- If the attack resulted in the access or acquisition of personal information, do you know what your legal obligations are under data breach notification laws?
- Have you considered whether your response will be protected by the attorney-client privilege?

PARTNERING WITH LAW ENFORCEMENT

- Do you know when to report the incident to law enforcement and to what agencies (e.g. CISA, FBI, Secret Service)?
- Have you established relationships with, or obtained contact information for, local law enforcement officials?
- Have you considered how a "law enforcement delay" may impact your obligations under data breach notification laws?