Executive Leadership: the Next Steps After a Ransomware Compromise

Every level of your business plays a part in ensuring that your data and financial assets remain secure. However, despite your security team's due diligence and your employees' intentions, what do you do when ransomware attacks your organization? The first 24 hours after becoming aware of an attack are the most important for any business leader.

Don't risk responding poorly during these integral hours: here are the most important steps to take in response to a ransomware attack:

01

Understand who to notify and how:

• All relevant employees. Every team member involved must understand their next steps. Make sure these are defined before an attack occurs so that they can be easily referred to.

• Law enforcement. Understand the pros and cons in advance of notifying law enforcement so you can make the right decision in the heat of the moment. If you decide to contact law enforcement, know how to contact the local police, your local FBI field office, and the FBI's Internet Crime and Complaint Center.

• Your members, customers, and donors. Should you post a notice on your website about the attack? Send an all-member blast email? Or is this something to keep under wraps? There is no correct answer for all organizations, and having a game plan and providing firm, timely instructions to your team on how to communicate will keep you in control of the messaging.

02

Check in on your IT Department and ensure they are defining several remediation scenarios with their timelines.

Be prepared to make these critical business decisions when handed scenarios that look like this:

• Option 1: Restore from Backups, 4 days of downtime, $5,000 labor cost estimate, 90% chance of success

• Option 2: Pay the Ransom, 1 day of downtime, $50,000 ransom demand, 75% chance of success

03

Implement your Business Continuity Plan.

Once your teams begin actioning the chosen remediation scenario, you can immediately start implementing your pre-determined business continuity plan to keep operations going while your IT systems are down.

04

Update Law Enforcement, Media Relations, and Insurance.

Make sure to keep all essential parties informed. This includes updating existing law enforcement reports, messages to your media relations team, and providing any new information to your insurance carrier about the incident moving forward.

Ransomware attacks can happen to organizations of all shapes and sizes. Ensure your teams are prepared by defining **incident response** and disaster recovery plans before you need them. If your organization would like to work with cybersecurity experts in developing the best plan for your business, don't hesitate to get in touch.

Talk With a Cybersecurity Expert

designDATA
IT Made Simple. Modern. Secure.

1425 K Street NW, Suite 500, Washington, DC 20005
T: 301-921-6696 **E:** cybersecurity@designdata.com