Cyber Attack Recovery Guide

10 actions to take immediately

HUB

#LetsDoSomething

Be prepared to take the right steps, in the right order.

When your data is held for ransom, time is critical. Taking these 10 actions in this order will help you through the most critical responses when you are under a ransomware attack.

1

CONTACT YOUR I.T. DEPARTMENT

The first step in recovering your data is to alert your IT department. Before you take any action, let the person who manages your network know that you have received a ransomware message. You should not forward or reply to the message, or engage with the hacker in any way.

2

DISCONNECT THE AFFECTED COMPUTER

Ransomware is a virus that can spread throughout your network, infecting other computers and even backup files. Disconnecting the computer from the Internet, by unplugging it, will stop the virus from spreading to other computers and taking down the internal network.

3

DOCUMENT ALL DECISIONS AND ACTIONS

Every cyber attack or data breach is unique. It's important to capture what you did and how you responded (e.g., clicked on an email "like" or replied to a hacker's request) to help the IT forensics team understand what has occurred, what was done and who was involved. Keeping track of dates, times and responses is critical to a thorough recovery.

4

NOTIFY YOUR INCIDENT RESPONSE TEAM AND SENIOR LEADERSHIP

Every company should have a team of specialists who are prepared to handle a cyber attack. These can include employees from the IT, communications, legal and accounting departments, as well as the board of directors. The incident response team should be able to quickly engage your company's incident response plan and carry out their duties as assigned. If you don't have an incident response team or plan, take the time to develop one before an attack occurs.

5

CONTACT YOUR INSURANCE BROKER

Your insurance broker can help guide you through a successful recovery and claims process. Under your cyber insurance policy, you will most likely have access to experts who understand the recovery process and ensure you have the resources to comply with notification obligations to affected parties, forensic investigations and public disclosures.

6

CALL YOUR PRIVACY ATTORNEY

Your privacy attorney is a key part of maintaining compliance with federal and state regulations that require you to notify anyone whose data was affected by the breach. Their guidance can help you understand your obligations for communication, credit monitoring and regulatory compliance.

7

ENGAGE I.T. FORENSICS TO INVESTIGATE THE CRIME

Identifying the source of the attack is a major component of data recovery. By tracking the virus path, the IT forensics team can show what files have been compromised, the length of time your system was compromised, and how extensive the damage may be. Oftentimes, a ransomware event occurs weeks or months after the hack. The forensics team will be able to assess the length of time the hacker has been in your system and the amount of damage to your data.

8

ACTIVATE YOUR BACKUP FILES/DISASTER RECOVERY PLAN

You can possibly avoid paying a ransom if you regularly back up your data and test it to ensure that the backup works properly. When a ransomware attack occurs, your files are encrypted and can only be released with a decryption code provided by the hacker. If you can remove the corrupt data from your network and ensure that your backup system is not compromised, you may be able to avoid paying the ransom altogether simply by reinstalling your backup files.

9

CALL LAW ENFORCEMENT

A ransomware attack is a crime and should be reported to the authorities. They will conduct their own investigation into the attack, which will be reported and tracked appropriately.

10

COMMUNICATE WITH AFFECTED INDIVIDUALS

Notification laws require that when you have a data breach, the people affected must be notified. Sharing the details of the attack, how you addressed it and what you plan to do going forward is an important part of external communication. Affected parties can include your clients or employees. It may also be necessary to hire a PR firm, and even a call center, to manage outside inquiries.

Looking out for you.
Looking ahead for you.

Now you know the critical response steps to take in the event of a ransomware attack. But remember, every organization is different, with unique vulnerabilities and needs. You may need to consider alternative or additional steps to limit damages and enable recovery.

Let's work together to develop a robust cyber insurance program.

Contact a HUB advisor today at:
hubinternational.com/cybersecurity

HUB

hubinternational.com