TIP SHEET:

WHAT TO DO AFTER A RANSOMWARE ATTACK

You've survived ransomware—now what? Make sure it doesn't happen again, using effective prevention and detection measures. Here are the most important things to do next:

THREAT HUNTING

First and foremost, make sure the attackers are truly out of your network. All too often, victims clean off the ransomware, without realizing that the criminals have a secret backdoor into the network. Don't get hit again. LMG's team of experienced professionals can proactively hunt for threats to prevent the same criminals from locking up your files again.

TWO-FACTOR AUTHENTICATION

Deploy two-factor authentication if you have not already, for both cloud accounts and remote access to your network. This will prevent a wide range of compromises, including ransomware. LMG can help you deploy 2FA, if you need assistance.

ASSESS YOUR CYBERSECURITY

Find the flaws in your cybersecurity before hackers do. Conduct regular penetration tests and vulnerability assessments.

BACKUPS

Verify that your backups are complete and ensure that you test them on a regular schedule (i.e. monthly). Talk to your IT provider for support.

VULNERABILITY MANAGEMENT

Ensure that all of your systems are kept up-to-date on software patches. Your IT provider can share detailed patch management policies and status updates. LMG's team can audit, if needed.

MONITORING AND LOGGING

Catch intruders quickly, before they have a chance to detonate ransomware. Make sure that your monitoring systems detect suspicious activity and alert immediately if an intruder is inside your network. LMG conducts Network Monitoring Assessments and Attack Simulation Testing that can proactively identify any gaps in your monitoring program.

TRAINING

Make sure your employees are trained to resist cyberattacks such as phishing emails. LMG provides on-demand awareness training, webinars, seminars, tip sheets, and other materials to support a fully-fledged cybersecurity awareness program.

UPDATE YOUR RESPONSE PLANS

Ransomware is always a learning opportunity. Take the time to do a post-mortem meeting with your team, and update your response plans to address any issues that came up, so you are better prepared. LMG's experienced professionals can take care of this for you if desired, so you can get it done quickly without adding to your staff's workload.

Ransomware is a difficult and stressful situation. We're sorry that you were breached, and we hope these tips help you move forward with even stronger cybersecurity.

If you have questions or need supplemental support, please contact us. We are here to help.

LMG SECURITY

145 W FRONT STREET
MISSOULA, MT 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support. Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855 | E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com