ACRISURE®

Limitless Growth Through Exceptional Partnerships™

How to Protect Your Organization from Ransomware

Second Quarter 2020

According to cyber security firm Emsisoft, 205,280 organizations around the globe reported experiencing a ransomware attack in 2019—a 41% increase over 2018. This fact not only illustrates that ransomware attacks are on the rise, but it also underscores the need for organizations to act to prevent such attacks from impacting their operations.

What Is Ransomware?

According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware is a type of malicious software cyber actors use to deny access to systems or data until a ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable. In some cases, data may be deleted altogether.

Ransomware attacks are particularly damaging, as they create massive business interruptions and can lead to significant reputational harm for the impacted organization.

Examine Your Ransomware Exposures

A strong commitment to cyber security is crucial to protect your organization from ransomware attacks. CISA recommends examining the following questions to determine if your organization is prepared to address the risks presented by ransomware:

1. **Backups**—Does your organization back up all critical information? Are the backups stored offline? Has your organization tested your ability to revert to backups during an incident?
2. Risk analysis—Has your organization conducted a cyber security risk analysis of the entire organization?
3. Staff training—Has your organization trained its staff on cyber security best practices?
4. Vulnerability patching—Has your organization implemented appropriate patching of known system vulnerabilities?
5. Application whitelisting—Does your organization allow only approved programs to run on your network?
6. Incident response—Does your organization have an incident response plan in place for ransomware attacks, and has it been tested?
7. Business continuity—Is your organization able to sustain operations without access to certain systems? If so, for how long?
8. Penetration testing—Has your organization or a trusted third-party attempted to hack your own systems to test the security of your systems and your ability to defend against attacks?

For more information on assessing your organization's cyber exposures, contact Acrisure LLC today.

CISA Warns Against COVID-19 Cyber Crime

According to the Cybersecurity and Infrastructure Security Agency (CISA), malicious cyber actors are taking advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. CISA is encouraging individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions:

- Avoid clicking on links in unsolicited emails, and be wary of email attachments.
- Do not reveal personal or financial information in emails, and do not respond to email solicitations for this type of information.
- Review CISA's tips on Avoiding Social Engineering and Phishing Scams for more information on recognizing and protecting against phishing.
- Review the Federal Trade Commission's blog post on coronavirus scams for information on avoiding COVID-19 scams.
- Use trusted sources—such as legitimate government websites—for up-to-date, fact-based information on COVID-19.

Consider sharing these tips with your employees to help keep your network secure.

Protecting Remote Employees From Cyber Attacks

Although implementing a work-from-home program can provide a wide range of benefits for your business, allowing staff to work remotely also comes with unique risks and challenges. Specifically, having your employees work from home can increase their vulnerability to cyber attacks, which could result in costly consequences for your organization. With this in mind, it's vital to ensure your work-from-home program is secure by utilizing top-notch technology and providing employees with adequate cyber security resources.

First, it's important to assess your workplace technology to ensure it possesses proper cyber security features to combat work-from-home risks. At a glance, your organization's software should have these key characteristics:

- **A virtual private network (VPN)**—Having a VPN allows your employees to utilize a private, protected network connection. VPNs provide numerous cyber security features, such as hiding users' IP addresses, encrypting data transfers and masking users' locations. If you don't already have a VPN, you are missing a crucial step in implementing a secure work-from-home program. If you do already possess a VPN, make sure it's fully patched.
- **Restricted access controls**—Remote work technology should be equipped with the same account access restrictions as your on-site software. Furthermore, you should only allow competent, qualified and trusted staff to have access to sensitive company data.
- **Anti-virus and malware protection**—To protect your system from cyber threats, it's critical that all remote work technology has the latest anti-virus, malware and firewall protection software.

After you have prepared your technology, it's time to provide employees with robust resources and training to ensure a secure work-from-home program. Consider providing staff training on the following topics:

- **Taking care of technology**—Encourage employees to log out of their devices when they are finished working for the day and store all workplace technology in a secure, protected location.
- **Utilizing personal devices**—If you allow staff to use personal devices for work purposes, be sure to enforce a Bring Your Own Device policy.
- **Conducting regular updates**—Make sure employees know how to conduct regular software updates on all workplace technology. If you allow staff to use personal devices for work purposes, ensure they know how to conduct software updates on that technology as well.
- **Detecting signs of phishing**—Educate your employees on how to detect phishing scams.
- **Reporting cyber concerns**—Ensure that remote employees know how to report any cyber concerns that they might experience. Staff should report these problems to their supervisors and the IT department, if needed.

For more cyber security strategies you can use to protect your businesses, contact Acrisure LLC today.