rubrik

CSPi Technology Solutions

Best Practices on How To Remediate a Ransomware Attack

OVERVIEW

To pay or not to pay? That is the question confronting the growing number of businesses hit by ransomware. According to the FBI, ransomware will be a $1 billion market in 2020[1]. If a strong ransomware remediation plan is not in place prior to an attack, paying a ransom can seem like the only option. And why do organizations pay? Recovery can be painful and time-consuming, and in many cases, the backups themselves can be compromised.

Organizations should not be forced to trade off paying a ransom and costly downtime. Instead, they should be able to rely on their backups to recover quickly and reliably. This requires developing and testing a strong remediation strategy before ransomware strikes.

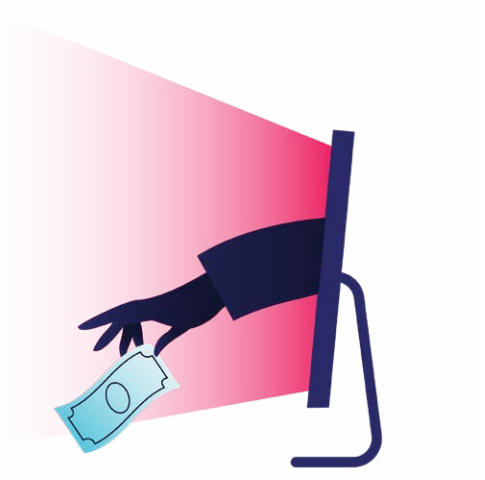
This guide will help you develop your ransomware remediation plan, so when an attack occurs, you can resume business operations quickly without paying a ransom.

HOW DO YOU ENSURE THE FASTEST RECOVERY POSSIBLE?

1. **Build and test a strong business continuity plan.**
    - Implement a holistic, cross-functional instant response team. Elect experts from the following areas: Network, Storage, Information Security, Business Continuity Management, and PR. Tailor this team to your own needs and expertise.
    - It is critical that you backup data regularly, verify the integrity of those backups, and test the restoration process to ensure it is working prior to an attack.
2. **Train your team.**
    - Run simulated exercises with your response team on a regular basis to test your ransomware readiness.
        - » Keep in mind how standard operating procedures differ based on region, business organization, etc.

YOU'VE BEEN HIT BY RANSOMWARE. WHAT NOW?

1. **Isolate the infected station from the network.**
    - Prevent the infection from spreading by disconnecting the network cable, Wi-Fi, Bluetooth, and all external storage devices such as USB or external hard drives.
    - Power-off affected devices that have not yet been completely corrupted to contain the damage.



1 Ransomware Prevention and Response for CISO

2. **Ensure backups have not been compromised.**

    - Backup data should never be available in read/write mode. Otherwise, it can be vulnerable to known protocols and easily manipulated or deleted by an attacker.

3. **Identify the infection.**

    - Investigate the type of ransomware you're facing, how it entered your system, and how it spreads in order to seal the breach.

        » Was it a phishing scam? Internet-facing vulnerability? Stolen user credentials? Your response may vary depending on the ransomware entry point.

4. **Determine your options.**

    - **Option 1:** Pay the ransom.

        » The FBI cautions against paying the ransomA. Paying a ransom does not guarantee an organization will regain access to their data. Ransomware victims may be subject to another attack or asked to pay an additional sum.

    - **Option 2:** Try to remove the malware.

        » It is questionable whether or not you can successfully remove an infection. Ransomware has become increasingly sophisticated and mutates frequently, making it less likely a decryptor is available.

    - **Option 3:** Recover from backups.

        » A strong backup strategy should allow you to restore from the most recent clean backup to avoid paying the ransom.

5. **Engage your incident response team.**

    - Notify the appropriate stakeholders to activate your business continuity plan.

6. **Diagnose the scope of infection.**

    - Quickly identify which files have been impacted and where they are located.

    - Visibility into how widespread the attack helps the incident response team recover only the impacted data and minimize data loss.

7. **Recover quickly.**

    - Restore your files to the most recent clean version of impacted data.

8. **Alert the authorities**

    - Inform law enforcement, customers, and any other necessary authorities. This is highly dependent on your business and industry.

HOW CAN YOU SECURE YOUR ENVIRONMENT FOR THE FUTURE?

1. **Implement security controls.**
    - After an attack, it is recommended to fix any identified vulnerabilities to ensure hackers can't re-access your environment.
2. **Strengthen your existing recovery plan.**
    - Use learnings from the attack to bolster your business continuity efforts. Adjust training exercises to help your team perfect areas of weakness and build off areas of success.

CONCLUSION

The most important step you can take to eliminate the pain of ransomware recovery is to have a backup and recovery solution you trust to keep your data secure. It is not a guarantee your backups will remain uninfected by ransomware, and recovery time varies immensely across vendors. Rubrik is the only solution with built-in immutability, impact assessment, and instant recovery, ensuring that your backups remain unaltered during an attack.

Don't wait for a cyber attack to develop your remediation plan. Check out Rubrik now.

CSPi Technology Solutions

182 East Newport Ctr Dr.
Deerfield Beach, FL 33442
United States
1-(800) 940 - 1111

CSPi Technology Solutions, provides the expertise and service scope - including Managed IT Services, Professional IT Services, and Cloud Services - to help our clients architect and manage a high-performance, highly available, and highly secure IT infrastructure. Our engineers are experienced in major industries and hold specialized industry certifications across networking, wireless & mobility, unified communications & collaboration, data center and advanced security technologies. Visit: www.cspitechsolutions.com

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit www.rubrik. com and follow @rubrikInc on Twitter.

20200310_v1