An Insider's Guide to
Ransomware Preparedness & Recovery

This IT guide provides actionable steps to reduce the impact of ransomware or other malware attacks. By quickly restoring data from time-indexed copies, organizations will be far less vulnerable to costly and debilitating ransom demands.

Your Data Held Hostage

Ransomware attacks have become the cybercrime du jour, affecting a growing number of organizations nationwide. An easy, low-risk way for criminals to exploit almost any network intrusion, ransomware is a **type** of malware attack that prevents organizations from accessing their own data or computer system until they pay a ransom to obtain a decryption key.

Ransomware is on track to become a **$1B** industry

According to a CNN report, ransomware events collected $209 million in Q1 2016, and are expected to collect $1 Billion in 2016. The FBI estimates that attacks using the CryptoWall variant of ransomware accrued over $18m by June 2015. And, in the first quarter of 2016 saw quadruple the attack rate seen whole of last year.

No industry is immune from ransomware attacks although some, such as **healthcare**, have **been especially hard hit.** An April 2016 ransomware attack at Maryland's MedStar Health hospital network forced 10 of its hospitals to operate without access to their central networks for more than a week. Following a ransomware attack in February 2016, Hollywood Presbyterian Medical Center paid $17,000 in bitcoin to recover its data.

With ransomware attacks on the rise, organizations of all sizes have found themselves vulnerable and struggling to reduce risk or respond to an attack.

Computing Conditions and Practices Open Door to Attacks

There are a number of security vulnerabilities that leave computing networks open to ransomware. Most incidents involve an unsuspecting individual clicking on an tainted link or e-mail attachment. Systems with out-of-date or misconfigured software can also be compromised to help spread ransomware. Windows systems have been the main target in the past but this is rapidly changing. According to the 2016 Symantec Internet Security Threat report, Macs and smartphones are increasingly affected, as are Linux systems, meaning that no computing platform is safe.

> “The widespread use of mobile devices by today’s workforce has also escalated the risk of malware attacks.”
>
> - Dave Packer, VP of Product Marketing, Druva

The widespread use of mobile devices by today’s workforce has also escalated the risk of malware attacks. While many companies are protected by a corporate firewall, employees are now connecting to enterprise data and services using their own weakly protected mobile devices. In fact, the 2015 Kaspersky Consumer Security Risk Survey found that 73% of employees report doing some work from their personal devices. This opens another route for malware to infect organizations and likewise, the deployment of unsecured mobile applications for employees and customers has created new opportunities for attacks.

The Cost of Inaction

Organizations may be tempted to cross their fingers and hope they won’t be targeted. Unfortunately, the chances of ransomware or other malware attacks are very high, with serious consequences for organizations that fail to take preventive action. In addition to paying a stiff ransom, victims may suffer costly business downtime and, in some industries like healthcare where ransomware attacks must now be reported as HIPAA breaches, fines and penalties for data breaches, not to mention a loss in reputation which can be very expensive in its own way. It likewise takes time and money to respond reactively to incidents when there’s no viable plan in place. Companies that pay the ransom to recover their data still face the threat of significant data loss if their files are altered during the decryption process. This is especially critical if an organization is under litigation, as it poses the risk for data spoliation and penalties. And don’t forget that not only do many victims of ransomware never recover their data even if they do pay the ransom, but many organizations have paid only to be re-targeted again.

Cloud Application Data (Office 365, Box, Google Drive) at Risk as Well

Organizations may think that their cloud application data is somehow immune to ransomware attacks and serves as a safe ground for that data, wherein the reality is they can actually make the problem more complicated by spreading the problem. Remember, most cloud application services operate based on a synchronization model; what changes on the local device within seconds begins copying over to the cloud application. As ransomware takes root and starts encrypting files, those files will be recognized as changed files and synchronized accordingly, posing a significant issue for shared project files and providing a vehicle to spread the malware more broadly.

Prevention Techniques Useful but Limited

Protecting the data perimeter is one approach to staving off ransomware and other malware attacks. End-user awareness and smart browsing practices are important, as is regularly updating security, anti-virus and anti-malware software, including operating systems. Because attackers benefit from weakly protected data, organizations should also replace antiquated IT infrastructures.

While these **fixes certainly play a role in preventing attacks, they have limitations** and provide only a weak and variable level of protection. No matter how updated your data protection scheme is, the malware attacks are getting smarter and attackers are finding new ways to penetrate. This means today's anti-malware vendors are playing a catchup game and there is always a vulnerability around the corner; it is just a matter of time till someone finds it and exploits it. In other words, ransomware attack is becoming more of an inevitability for many organizations.

Another weakness is that user awareness relies on the compliance of busy and increasingly mobile employees to prevent ransomware attacks that are ever-more convincing and difficult to detect. While offering some protection, encryption doesn't help if users inadvertently download a virus or malware onto their computing device. In addition, ransomware is often designed to stay dormant after spreading through networks, making it harder to identify the original source. Given the major gaps in protection afforded by malware prevention techniques, organizations would be foolhardy to rely on them exclusively.

Data Backup Thwarts Ransomware, Provides Other Benefits

Experts agree that a comprehensive data protection plan is the best defense against ransomware and other incidents of malware, and backup plays a critical piece in thwarting ransomware attacks. According to Gartner, "The primary defense for ransomware infections (and potentially future coordinated attacks) is backup."

Gartner recommends implementing end user backup, as well as setting recovery point objectives (RPO) for servers at risk for ransomware (such as Linux web servers). Automated and time-indexed snapshot backups of data across servers, laptops, and cloud apps enable the restoration of information back to its original state, and as a result, organizations can access their data from any point in time prior to the attack.

It's easy to see how a solid backup plan improves an organization's security and negotiation stance when confronted with an attack. Enterprise-grade data backup also provides several major benefits unrelated to ransomware, whether the data loss stems from malware, system failures or human error. The right data backup solution facilitates better information governance and gives organizations the ability to view audit trails and protect data for compliance purposes. A cloud-based backup solution also provides critical off-site storage when on-premise data is at risk.

A 6-Step Plan for Data Backup

Druva's data protection experts have outlined six proactive steps that IT can use to keep data safe. These steps provide the foundation of a backup plan that is highly efficient, seamlessly executed and unnoticeable to the end user.

1. **Protect Distributed Data: "How"**
   An enterprise-grade automated backup solution that performs regular backups across devices, desktops and cloud apps will protect distributed data and act as an insurance policy in case of a ransomware strike or other intrusion. Make sure to select a cloud-based backup solution, as it provides off-site storage. Off-site storage that leverages any of the AWS or Azure storage locations not only provides off-site capabilities but also complies with local data residency laws by storing it in the same region.

2. **Backup Distributed Data: "Who"**
   Does your current backup plan cover 100% of your user base, including geographically distributed teams? To reduce your exposure to potential data loss, review and validate the deployment scope of your backup plan to ensure that your backup solution deploys automatically to all end users needing protection. At a minimum, you should ensure that key users are covered by your data protection policy.

3. **Review the Scope of Your Data Backup: “What”**
   What are you backing up? You’re probably protecting desktops and email, but what about other user-specific data sets such as profiles, system and app settings, or folders? We highly recommend that you review, validate, and, as needed, modify backup content to ensure that all important data for protected users is backed up. If you need a more comprehensive plan, you should consider creating custom folders where users can store data for backup and further reduce data loss.

4. **Check Backup Frequency Across Distributed Teams: “When”**
   How often are you backing up? Every 2 days? 8 hours? 4 hours? Do you need an even more aggressive schedule for executives? Review, validate and, if needed, modify backup frequency to ensure automated, periodic backup of mission critical data for all protected users. As a general rule, we recommend that you backup data, at minimum, once every 4 hours, and every 2 hours for key users. You may also want to select a different backup frequency depending on the requirements of specific users and teams.

5. **Validate Your Retention Policy: “How Long?**
   How long are you keeping your backups? 14 days? 7 weeks? 6 months? Review, validate and, if needed, adopt a longer retention policy to meet internal objectives and ensure a sufficient RPO, especially for key people and departments. Your data retention policy may vary depending on your industry, regulations and internal IT policies. IT, Legal, and Compliance teams may need to weigh in on data retention needs. For ransomware purposes, given dormancy periods, start thinking in the 3+ month timeframe.

6. **Re-Assess Policies Periodically: “Looking Ahead”**
   While the preceding measures might provide sufficient protection for the foreseeable future, we highly recommend that you revisit your backup policies approximately every six months to ensure that they meet your organization’s needs. IT often has the primary responsibility for this routine and, in some cases, acts in coordination with the Legal team.

How Druva inSync Can Help

Rated as the industry's #1 enterprise end-user data protection solution, inSync from Druva can help IT teams recover from a ransomware attack by ensuring thorough backups before the event. Designed for endpoints (e.g. laptops, desktops, smartphones, tablets) and cloud applications, Druva inSync provides an automated, enterprise-grade backup solution to quickly restore data in case a network or end user is compromised - even if the hardware is locked forever. Specifically, inSync offers:

Automated Time-Indexed Backups: inSync offers time-indexed, snapshot backups of user data and user-specific system and app settings so that data can be easily returned to its original state before the attack.

Immediate Data Access: inSync providers customers with immediate access to data from anywhere so that users are never impacted by ransomware or other malware, ever.

Frequent Backups: inSync enables organizations to backup data as often as every 5 minutes.

Multi-Zone Redundancy: inSync's data center with multi-zone redundancy provides the highest level of data reliability and guaranteed availability to ensure business continuity.

Greater Storage Options: To best meet their data storage, privacy and security needs, inSync provides customers with greater choice (AWS or Microsoft Azure) for global storage options as well as choice regarding their preferred infrastructure vendor.

Covers Mobile Devices: Mobile devices outside the firewall are a target for introducing malware. Backing up data on endpoints is a must, and inSync provides coverage by backing up data on endpoints as well.

User Friendly: inSync is optimized to ensure successful backups and restores, even on varying network speeds, with zero impact to users.

User-Added Folders: To ensure that all key data is protected, inSync allows end users to add folders and self-select the data for backup. End users can also self-restore their data, along with personal and application settings from any new device.

Conclusion

By following the steps outlined in this IT Guide and selecting Druva's inSync as its enterprise solution, IT can ensure that it has a rock-solid backup routine in place to reduce the impact of ransomware or other malware attacks. Armed with the ability to quickly restore data from time-indexed copies, organizations will be far less vulnerable to costly and debilitating ransom demands. Who needs weeks of drama and negative headlines when industry-leading cloud backup is available?

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information – dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

Druva, Inc.
1 888-248-4976
sales@druva.com
www.druva.com