



Resolving Ransomware Incidents with Disaster Recovery-as-a-Service

As well as other cybersecurity threats

The Struggle for IT Resiliency

A single ransomware attack can halt an organization with sophisticated encryption methods that make computer networks and files inaccessible. When IT departments and business leaders don't act fast in this scenario, they risk losing critical data forever and ending up with a significant reputational impact if news of the breach leaks to the public. **This leaves victims with an immediate decision: 1) Pay the ransom for data back, or 2) replace the encrypted data with clean copies.**

Companies with no copies of data must pay the attacker's fee if they want to get out of the situation without data loss. The problem is that this only perpetuates the cycle of cyber criminality, as it feeds into the multi-billion-dollar industry of ransomware. Worse, those who pay the ransomware fines are susceptible to future attacks, as word spreads within the cybercriminal community that they were willing to pay. Plus, just because you pay the fee doesn't mean you'll actually receive the key to decrypt your data.

Perhaps this is why, in [a 2017 survey](#) across six major industries, 51% of executive leadership and IT managers rated ransomware as the biggest security threat to their organizations.


Why ransomware is a growing threat

Different from other forms of cybersecurity events like malicious probing or malware infections, ransomware criminals aren't primarily focused on information theft. In fact, they tend to have little interest in the data itself, so long as it's sensitive and urgent enough to prompt payment from the victim. Attackers have gotten sophisticated in selecting lucrative industries that have a stigma of legacy or inadequate infrastructure (such as government, healthcare or legal). When notifying these businesses, cybercriminals often do so with the assumption that the IT department has no recent backups and will pay the fine rather than lose data and valuable time.

Industries with sensitive data are especially susceptible to ransomware attacks—and where there is sensitive information, there may be compliance responsibilities as well. For example, the legal industry is subject to [regulations and a code of conduct](#) that requires firms to allocate their resources appropriately to manage risks and protect their clients' assets. If a ransomware breach compromises data under compliance, law firms may need to pay regulatory fines too.

Widespread threats are changing the make-up of IT departments

The evolving threat landscape, for all cybersecurity events not just ransomware, is bringing IT



"Customers and clients want to know that you're going to prevent unwarranted access to their sensitive information. So, if you end up in the news with a catastrophic ransomware attack this will make them uneasy - and significantly hinder their retention. Also, it should go without saying that fleeing customers will impact the acquisition of new ones."

– Jeff Ton, EVP of Product & Service Development at Bluelock

roles for disaster recovery (DR) and cybersecurity together. Historically, these two groups would have covered their respective specialties and seldom worked together. But now, given that security professionals have long been known for their quick incident responsiveness and DR professionals are committed to avoiding data loss, companies are recognizing the value both realms have in preserving overall business continuity. This means that company leadership is increasingly asking DR and security professionals to join forces for full IT resiliency – which doesn't just mean working cooperatively. **IT security requires a two-pronged approach to mitigate risk: [an equal balance of preventative and restorative measures](#).** Bridging these two important focuses, threat detection is also a critical component, since it helps to identify when a breach has occurred.

How to tackle ransomware with DRaaS

Companies have long been using [Disaster Recovery-as-a-Service \(DRaaS\)](#) to solve for downtime and data loss. But now that more [companies are formally considering security incidents disasters](#)—and rightly so, given the similar impacts on data loss, downtime, reputation, etc.—people are looking at DRaaS as a mitigation solution for cybersecurity.

Why DRaaS for ransomware

In the case of ransomware, where every second is lost money, **organizations need to have a DR strategy in place that can bring them back online within minutes to hours, not days.** For organizations relying on tape backups, for instance, the inconvenience and complications that can occur due to the days that it will likely take to restore systems may lead to preferring to pay the ransom.

DRaaS offers recovery points of seconds-to-minutes with a faster recovery time, pairing continuous data replication and backup-based replication together for a full mitigation strategy. When a ransomware attack happens, you have more recovery options to locate the most recent clean copy of your data. Plus, depending on if you have a fully-managed or assisted model of DRaaS, you may have access to a team of experts who will help mitigate the situation after a breach (ideal for overburdened IT teams).

Three Types of DRaaS:



Self-Service DRaaS

You get the tools to assemble your DR plan yourself



Assisted DRaaS

You get the tools to assemble your DR plan yourself with DRaaS experts available for advice and assistance



Managed DRaaS

DRaaS experts assemble your DR plan and manage all maintenance

With DRaaS, the focus is getting an entire workforce returned to normal. Due to the complex business processes involved in a system restore, simply retrieving data is insufficient. For this reason, a company must not only have policies to retrieve and restore compromised data, but also have alternative means for employees to access the recovered data and systems at the DR site. Most companies tend to encounter problems in an event when they've not regularly tested connectivity scenarios for post-failover access.

What to do after a ransomware attack using DRaaS

- Refer to your playbook and contact your experts

First, initiate your response plan, as detailed in your DR playbook. Notify your leadership, public relations, cyber forensics experts (to lead an investigation), cybersecurity legal counsel, insurance provider and – perhaps most importantly – call your DRaaS provider to be on high alert for failover.

- Pause and make a decision

In most cases, it is best to pause all replication and/or backup solutions so that you can prevent the intrusion from spreading pervasively across all IT systems. Potentially, you may want to keep a portion of your infected environment running to preserve evidence for a criminal investigation.

Don't do anything in terms of recovery execution until you know the full extent of the damage, since restoring your IT systems with infected versions of your data will only be a waste of time. Make a decision whether to do a full or partial failover, or to simply repair a single infected application.

- Execute your recovery process

When your company is ready to proceed with the recovery execution of your IT systems, the goal is to locate the most recent clean copy of your applications and data. With cloud-based replication, you have several snapshots of data to look back at, all within seconds-to-minutes of each other. If your replication solution doesn't have a clean copy, then you should look to your cloud-based backups, which typically have a longer retention period.

Once you have the newest clean copy of your IT systems, stand it up in a separate offsite environment (if possible) and run business operations out of this location until your cyber forensics experts have everything they need from the ransomware-infected production environment for criminal investigation. Before returning all functions to your normal production site, it may be good to test the new environment in its failed-over state first—to ensure everything has been resolved.



STEPS TO RANSOMWARE RECOVERY WITH DRaaS

1. Initiate your incident response plan

2. Contact your experts

Notify the following:

- Your cybersecurity legal counsel
- Cyber forensic experts to lead an investigation
- Your IT-DR provider to take action or be on high alert for failover
- Public relations

3. Halt replication and/or backup

Do not propagate issues into recovery environment to ensure you don't lose clean data

4. Make a decision

Should you failover the environment or can you simply repair one application?

5. Initiate recovery or restoration

- Find the most recent recovery point prior to the attack to reduce data loss
- If possible, recover your environment at an offsite location to preserve evidence available in your production environment.



Key takeaways

Keep in mind that no solution will truly prevent ransomware, so the ability to recover takes precedence. DRaaS offers an offsite location to recover a clean copy of your data in, rather than restoring systems in your production site and risking lost forensic evidence. Plus, DRaaS allows for greater speed in locating the right copies of data, and recovering them with minimized loss.

According to a recent [Bluelock-commissioned survey](#), executive leadership tends to care more about time-to-recovery and IT managers tend to care more about data loss. This is just another reason to use DRaaS as part of your overall security incident response plan, since it solves for both priorities.

The recovery point makes all the difference when ransomware strikes, and DRaaS can give you the most granularity and widest range of options (for example, you can roll back to a backup if the intrusion wasn't caught fast enough). DRaaS functions as a mitigation strategy not just for ransomware, but for any security breach. A provider like Bluelock will guide your company through how to formally consider security events "disasters" and treat them with the same urgent attention, so that you can fully integrate DR and cybersecurity practices into your company's wider business continuity strategy.

Why Bluelock

Because of Bluelock's commitment to the success of your business no matter the event, we offer both assisted and fully-managed DRaaS models, so you can select the perfect level of involvement for your company's existing resources and objectives. [Our solutions](#) are always tailored to match your unique security, complexity and compliance needs, since DR and cybersecurity are never one-size-fits-all and leave-it strategies.

Unlike any other DRaaS provider, Bluelock offers a [Recovery Assurance™](#) program to all of our Managed DRaaS clients for complete confidence in the solutions you've purchased. Not only do you get a second pair of expert eyes with robust firewalls, patching and constant monitoring of your IT systems, you'll also get the most comprehensive service level agreements (SLAs) in the industry for guaranteed responsiveness and recovery.

[Contact Bluelock to learn more.](#)

A DRaaS PROVIDER EMPOWERS CYBERSECURITY

- **Segmented networks in an offsite environment**
- **Testing and documentation to make sure protection practices stay up-to-date**
- **Ongoing monitoring and encryption**
- **Team of experts for methodology, maintenance and recovery execution (ideal for overburdened IT teams) - different levels of managed services exist**



www.bluelock.com | 888.402.2583 | Indianapolis • Las Vegas