A ransomware attack is a classic ticking-clock scenario. Your critical business data has suddenly been taken hostage. Hackers have used advanced encryption to render it inaccessible — and now they’re demanding an exorbitant amount of money to decrypt it. How will you respond? Can you ensure the safety of your data if you refuse to pay — or even if you do? While you consider your options, your organization remains paralyzed. Every passing minute increases the pressure to make the right choice.

This scenario has already struck companies of all sizes across industries around the world. Yours could be next. Are you ready?

In this guide, we’ll explore the ever-evolving threat of ransomware — and what you can do about it. First, we’ll examine ransomware as one of the many threats to recovery readiness facing today’s organizations. We’ll then drill deeper into the nature, impact, and direction of this insidious form of attack. Pivoting from awareness to empowerment, we’ll then explore risk management elements, including planning, prevention, monitoring, fast restores, and testing. Finally, you’ll learn how recovery readiness can keep you from becoming a victim by providing a critical last line of defense against ransomware.

Your stand against ransomware begins now. Read on.

**Threats to recovery readiness**

Recovery readiness means being in a position to restore your organization’s data and applications quickly, no matter what happens. In today’s diverse IT environment, that’s a major challenge. First, you need to understand threats to backup data can come in many forms, both inside and outside the company.

**Internal threats**

People often think of a “threat” as something intentional and malicious. That’s usually the case, such as when someone intentionally deletes data because of a grievance against their organization. That’s what happened to one U.K. company’s AWS accounts in 2019. An internal threat might also originate with an outsider who has acquired credentials through theft, blackmail, or manipulation and uses these for ill intent.

But internal threats can also be accidental. An employee with legitimate access might simply click the wrong button and leave data exposed, or delete the wrong entity, and do untold damage to the organization. This almost happened to AWS itself in 2020, when one of its engineers inadvertently leaked his passwords and cryptographic keys to various AWS environments — though in this case, an outside analyst alerted the company before any damage was done. People are human; it happens.

**External threats**

External malicious actors are, in simple terms, bad guys. They’re hackers or other individuals seeking to infiltrate your organization for their purposes. Making money is a substantial motivating factor for malicious actors. For example, cryptojacking has become a popular method of stealing compute resources within an organization for mining cryptocurrency. Malicious actors may also be motivated by political or competitive reasons, with a goal to delete data, leak data, or disrupt business services.

Whatever their intention, they use password spraying techniques to gain unauthorized access into an organization or system. Or they might try to exploit vulnerabilities, inject botnets and rootkits to steal, and delete data or disrupt an organization’s ability to function.
That’s where ransomware comes in. In a typical attack, the hacker uses malware, often delivered via an infected attachment or link in an email, to encrypt your data. As in a flesh-and-blood ransom situation, the hacker then demands payment — or you’ll never see your data again. Without an effective recovery readiness strategy, your only option is to pay up and hope for the best.

The high cost and rising threat of ransomware

There’s a reason ransomware makes the headlines. It’s the kind of attack that gets your attention — it’s sudden, brutal, and leaves the victim feeling helpless. In recent years, the rapid rise of ransomware has cast a shadow of anxiety across organizations.

Alarmed business, IT, and security leaders aren’t just being paranoid. In a Black Hat USA 2019 survey, 65% of respondents believe they will have to respond to a major security breach in their organization in the coming year, up from 59% in 2018; most do not think they have the staffing or budget to defend adequately against current and emerging threats.1

And the impact can be devastating.

• In 2017, FedEx reported that a cyberattack had cost them $300 million. And that’s not from paying the ransom — in fact, none was collected by the attackers. Instead, this represents the cost of system downtime and disaster recovery following the attack.
• Municipalities face similar risks. Since getting hit by the SamSam ransomware in March 2018, the city of Atlanta, Georgia, has spent more than $5 million rebuilding its computer network, including spending nearly $3 million hiring emergency consultants and crisis managers.
• Currency dealer and travel money services provider Travelex was hit by ransomware over the critical holiday travel season at the start of 2020, taking its global websites offline — and forcing employees to revert to pen-and-paper methods at 1,200 locations across more than 70 countries. Travelex partners, including Royal Bank of Scotland, Barclays, Tesco Bank, and Asda felt the impact as well.
• No target is off-limits for hackers. In October 2019, DCH Health System in Alabama was forced to pay an undisclosed ransom after hackers locked the IT system serving three hospitals. Patient care continued under emergency procedures, but incoming ambulances had to be diverted elsewhere whenever possible.

When something works, hackers keep doing it — and keep getting better at it. As ransomware technology and practice continue to grow in sophistication, criminals will squeeze as much money as possible from any victim they can find. Here are a few more alarming considerations:

• Think you’re safer on a non-Windows platform? Ransomware including Lilocked, B0r0nt0K, HiddenWasp, and QNAPCrypt began targeting Linux systems in 2019, with further attacks sure to follow.
• Apple fans need to stay on their toes as well — Macs are just as susceptible to ransomware as any other platform, and incidents are already on the rise.
• Cybersecurity Ventures predicts ransomware will cost $6 trillion annually by 2021. That’s more than the GDP of Japan.

Fighting back — or trying to

Common countermeasures to ransomware include antivirus, antimalware, and firewall blockers. These are certainly necessary, but they’re not enough to keep you safe. In fact, the majority of victims already had these solutions in place. That means your ransomware strategy should reduce attack risks while also seeking to mitigate the impact of an attack that succeeds anyway. It’s all too likely that one will — so you need to be ready.

Ransomware: 4 ways to protect and recover Read >
Learn how to protect against ransomware and manage risk

A complete ransomware strategy includes reducing the risk of a successful attack and lessening the impact of an attack that does succeed. There are five things you need to do: plan, prevent, monitor, restore (quickly), and test.

1 Create a plan

An ongoing attack is no time for improvisation or ad hoc measures. An effective plan is a foundation for a full and speedy resumption of normal operations. An anti–ransomware plan’s essential elements — like any disaster recovery plan — are what, when, and who.

• What – Identify and prioritize critical applications so you can focus first on the systems and data that you’ll need to recover first.

• When – Define the Recovery Point Objectives (RPO), Recovery Time Objectives (RTO), and Service Level Agreements (SLAs) for your systems, data, and applications. How soon is soon enough to recover? How far back do you need the restore to go? Based on these metrics, you can then perform an internal assessment and identify existing gaps in your recovery capabilities. Are there systems or data you’re currently unable to recover effectively within the specified parameters? This will help you understand whether you’re adequately prepared for a ransomware attack or if there’s more work you need to do.

• Who – Which players – internal and external – will be involved in your data recovery efforts? How will they be notified? What conditions will trigger an escalation, and to whom? Your cast of characters should include both internal IT and line–of–business personnel and external suppliers and vendors with a relevant role to play.

As you make your plan, you should also decide whether to leverage third–party recovery readiness expertise and resources. An expert partner can provide recovery readiness assessment services through implementation, monitoring, management, and response.

Disaster recovery planning for today’s real–world outages Read ›

2 Prevent attacks

While it’s not realistic to try to make your organization completely invulnerable, every attack you can prevent will save you tremendous pain, time, and cost. There are several ways to go about this.

Start with user vigilance. Most ransomware — and most malware in general — is delivered via email and triggered by an unsuspecting employee. Preventing this can be as simple as making sure attachments have come from a known sender or trusted source before opening them. Similarly, software should be downloaded only from a legitimate vendor or app store and scanned for malware before it’s clicked. Measures as simple as these could have stopped many high–profile breaches.

IT needs to act responsibly as well. Updates and patches should be applied promptly — most successful attacks exploit vulnerabilities for which patches have long been available. Sound IT practices are non–negotiable.

Once you’ve reduced the risk of malware entering your environment, the next step is to secure and protect your data against any exploits that succeed. This should include:

• Foundation hardening – Vulnerabilities and configuration flaws in your operating system, database, application, and web server technologies can provide an entry point for all types of cyberthreats. For example, you should disable the use of Server Message Block 1 (SMB 1), which does not support encryption. Hackers can use these vulnerabilities to compromise your data protection platform’s integrity and put your backups at risk.

• Application hardening – Being able to access your applications directly makes life a lot easier for a cybercriminal. Use the AAA Security framework as a guideline for protecting your applications: Authentication, Authorization, and Accounting.
### AAA Security framework for controlling access

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proving and granting access</td>
<td>Control what level of access is required</td>
<td>Tracking and auditing access and capabilities</td>
</tr>
</tbody>
</table>

For authentication, Commvault integrates with secured LDAP-based directory services and external identity providers via OAuth and SAML protocols. Additional measures include support for two-factor authentication, encryption for credentials and impersonation accounts used for backups, certificate authentication, and Zero Trust controls to protect against threats originating from inside the network.

Fine-grained authorization controls the level of access granted to authenticated users based on their roles and needs. A passkey can be required to perform restores, while a data privacy lock can restrict browse and restore operations to the data owner or other select parties.

Accounting includes tracking and auditing users’ data access and capabilities regularly. Unnecessary privileges should be removed, while data encryption should be routinely audited.

### Ransomware protection
- Make sure the backups in your data protection platform are as safe as possible. This includes keeping the platform itself from being a conduit to spread malware to the backup data it holds. (Keep in mind that your data protection platform isn’t designed to scan for or remove malware or to prevent it from spreading to backup data from external sources.) There are several ways to protect backup data, each with its advantages and challenges.
  - A backup appliance can harden your architecture with vendor-supplied hardware. This can be a good idea — though you’re counting on the vendor to provide regular updates to maintain its effectiveness.
  - WORM (write once, read many) technologies can block illicit encryption attempts by making backup data immutable — in other words, impossible to change or delete. Immutability protects data both within and outside the backup solution. Just make sure it won’t pose barriers to the recovery objectives you’ve defined.
  - Data isolation using air gap techniques can reduce the exposure of backup data to the risk of malware. If there’s restricted network access or read/write access to backup copies of your data, there’s no way to breach or corrupt that data as only verified backup processes can manage those resources. To be effective, you should also consider physical access to data — there’s still the possibility of an insider inflicting physical damage to your storage library.

### Monitor your environment

No matter how consistent and effective your countermeasures are, you have to assume that at some point, ransomware will enter your environment. At that point, the focus shifts to monitoring: detecting the attack as quickly as possible so you can reduce its impact.

Detection can include scanning servers for anomalies such as unusual file system behavior that can signal that an attack is underway. Machine learning has become a key asset in this effort, using historical data to recognize the difference between legitimate activity and potential trouble signs.

Honeypots take detection one step further by creating a hidden file of a type that’s especially appealing to hackers and monitoring it for signature changes and other anomalies.

Centralized management and reporting are essential to identify gaps and take proactive action. The IT team should have a single screen to watch for anomalies such as modifications and deletions in file system metrics or the backup index. When potential indicators of ransomware or other threats have been detected, real-time alerts can trigger a rapid response through integration with ticket systems or by initiating workflows.

Protecting your environment from a ransomware attack with Commvault [Watch »](#)
4 Restore your data

Fast restores can greatly reduce the impact of a ransomware attack. Not only do you still have an intact copy of your data — you also can make it available to systems and users quickly so you can resume normal business operations.

There are three ways to backup data, each with different implications for restoration.

• Traditional backup operates at the file level. The system works through all the files and directories in the volume to determine whether they've changed and need to be part of the current backup. This can be a time-consuming and resource-intensive approach, though, as the system has to navigate every aspect of the index — an aptly named "tree-walk."

• Block-level backup avoids the performance penalties of traditional backup by working on a block-by-block basis. The application doesn’t care how many files there are or what your index looks like. That allows faster, more efficient backups, making it feasible to perform backups more frequently.

• Replication takes a continuous approach to data backup. One way to do this is through continuous data replication (CDR), which involves logging all file write activity on the source computer, transferring this log to the data recovery platform, and replaying it to create a near real-time replica. Another option is to use incremental replication to continuously apply changes from a source backup to a backup synced copy. Volume block-level replication (VBR) is often the best approach, combining block-level backup efficiencies with the near real-time advantages of replication. This allows granular point-in-time recovery, crash-consistent recovery points, application-consistent recovery points, and effective recovery point lifecycle management.

5 Test your plan

Once you have your plan in place, along with the procedures and technologies to execute it, make sure it’s going to work as needed. Perform frequent tests to verify that you can meet the SLAs you’ve defined for critical and high-priority data and applications. Your system should be able to report on metrics such as RPO, actual recovery point, RTO, and estimated recovery time for each of your protected systems. As you identify gaps in your readiness, incorporate the appropriate adjustments into your plan for improvement. For a practical and sustainable testing strategy, you should be able to test your recovery capabilities in real-time without impacting staff or business interruptions.

Testing can be an excellent area to bring in additional third-party resources — especially if your IT team lacks the bandwidth or expertise to perform regular quarterly reviews. An expert partner can provide services such as estimating your disaster recovery settings and operations’ effectiveness, validating your backup data integrity, alerting you to systems that will miss SLAs, and providing recommendations for corrective action.

Taking action against ransomware

Your Commvault data protection and recovery solution can be a valuable part of your anti-ransomware strategy. Advanced technologies powered by artificial intelligence and machine learning make it possible to detect and alert on possible attacks as they happen so you can respond quickly. By keeping your backups out of danger and making it possible to restore them quickly, you can minimize the impact of even a successful ransomware attack so you can get back to business right away.

A TechValidate survey conducted in June 2020 illustrates the difference Commvault makes for customers. Of the organizations surveyed:

• 95% said Commvault gives them greater confidence in restoring their data to quickly resume business operations.²
• 82% have benefited from improved protection of critical data with Commvault.³
• 74% have benefited from improved restore times (Recovery Time Objectives) with Commvault.⁴
• 90% agreed: "Commvault has expanded our disaster recovery capabilities."⁵
• 84% improved preventing data theft or breach by 41 – 60% with Commvault.⁶

---

2 TechValidate survey, https://www.techvalidate.com/tvid/217-244-928
4 TechValidate survey, https://www.techvalidate.com/tvid/03F-689-701
5 TechValidate survey, https://www.techvalidate.com/tvid/126-B60-61A
The State of Colorado used the Commvault platform to recover quickly and fully from a major ransomware attack against its Department of Transportation. In fact, the State first learned of the attack through a Commvault alert — before any of its dedicated security tools had detected the breach. A coordinated response plan across agencies, personnel, and technologies statewide helped immeasurably. Watch >

The City of Sparks, Nevada was hit with ransomware that locked its police department shared files and left crucial geographic data inaccessible by agencies across the city. In the past, unreliable backups had raised fears of data corruption, but with Commvault, the city achieved complete data recovery in only 12 hours. Watch >

Opportunity and risk— that’s the reality for businesses today and the people responsible for the data. A single event can threaten the bottom line or define a career. So how do you prepare? By making sure you’re ready.

There’s never been a more crucial moment to get your security on with Commvault. For more info, visit commvault.com/ransomware >