ConversationalGeek

RANSOMWARE RESILIENCE:

Backup Is Your Last Line *of* Defense

Data Protection's Role in Mitigating Ransomware Attacks

www.conversationalgeek.com

Sponsored by
Quest

Ransomware Today: The Good, Bad and Ugly

Here's some bad news…

As of 2023, 72 percent of businesses had been impacted by ransomware, and nearly three-quarters of companies that suffered a ransomware attack paid the ransom – often because they lacked backup data, and therefore had no alternative but to pay a ransom.[1]

Now, here's some even worse news…

Ransomware is poised to cause even more harm over the coming year and beyond. As Dan Lohrmann writes in Government Technology, "Ransomware threats will continue to increase and evolve in 2024."[2] Threat actors will devise new methods of attack that evade standard defenses, while also adopting increasingly aggressive tactics – such as compromising not just production systems, but also backup storage, which they'll also hold for ransom in a bid to prevent businesses from recovering without paying up.

But don't worry (too much), it's not all doom and gloom…

Even in an era when the typical organization struggles to stay safe from ransomware, it is possible to implement strategies that effectively mitigate the threat that ransomware poses to business success and longevity. Lest it sound like we're sugarcoating a pervasive problem, we should make one thing clear: Totally preventing ransomware attacks is not realistic. While you can and should invest in defenses, there's simply no way to guarantee a breach will never occur.

Your ransomware survival guide

What you can do, however, is take steps to ensure successful recovery from a ransomware attack if (or when) it does take place. This is the critical area where many businesses fall short. They overinvest in defenses – which, beyond a certain point, deliver diminishing value – and underinvest in the data protection and recovery solutions they need to be able to survive a ransomware attack without paying the ransom.

To prove the point, this eBook dives into the current state of ransomware threats and what businesses must do to protect themselves. As you'll learn, steps like hardening production systems against attack, and possibly even investing in cyber insurance, are important. But ultimately, you need to ensure that you have the data protections in place to serve as an effective last line of defense if your other mitigations prove unable to stop the ransomware attackers – which they inevitably will, sooner or later.

[1]"Annual share of companies worldwide that paid ransom," Statista; "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," chainalysis.com.
[2]"The Top 24 Security Predictions for 2024," GovTech.com.

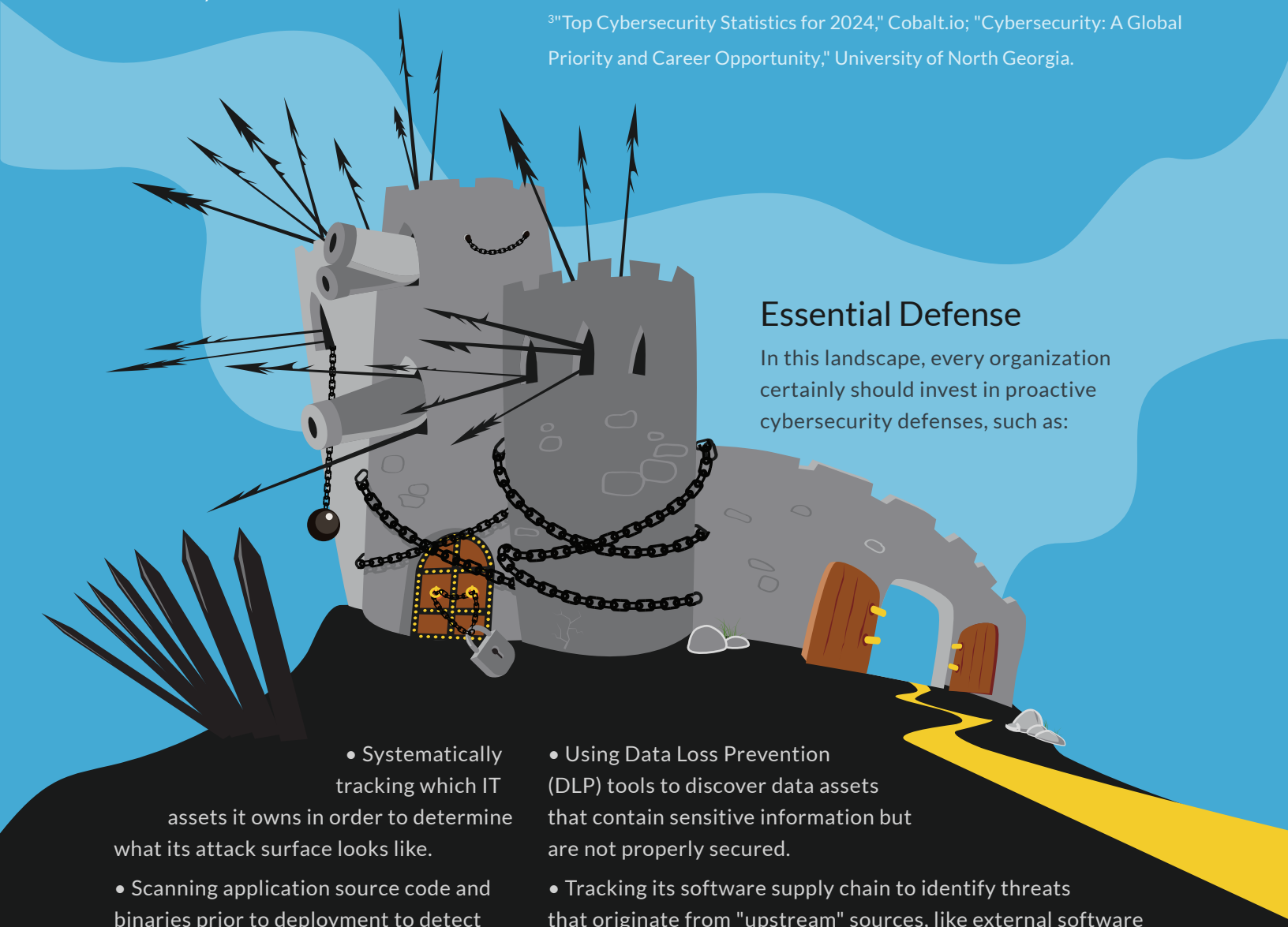
The False Premise of

ATTACK PREVENTION

Much of the conversation in the realm of cybersecurity today centers on stopping attacks before they occur. Businesses are told they need to take a proactive approach to security and adopt "shiftleft" practices – which means performing security scans and checks as early as possible, rather than waiting until attacks are underway to discover a risk.

That's all well and good. The old saying that an ounce of prevention is worth a pound of cure certainly holds true in the realm of cybersecurity. And indeed, given that on an average day, there are more than 2,000 cyberattacks and about 3.8 million records stolen, doing as much as you can to stay a step ahead of attackers is absolutely critical.[3]

[3]"Top Cybersecurity Statistics for 2024," Cobalt.io; "Cybersecurity: A Global Priority and Career Opportunity," University of North Georgia.



Essential Defense

In this landscape, every organization certainly should invest in proactive cybersecurity defenses, such as:

- Systematically tracking which IT assets it owns in order to determine what its attack surface looks like.
- Scanning application source code and binaries prior to deployment to detect vulnerabilities before the apps are in production.
- Performing penetration testing to identify overlooked gaps in cyber defenses.
- Using Data Loss Prevention (DLP) tools to discover data assets that contain sensitive information but are not properly secured.
- Tracking its software supply chain to identify threats that originate from "upstream" sources, like external software vendors and open-source projects.
- Monitoring vulnerability databases, such as the NIST NVD databases, to track newly discovered security risks and evaluate whether they impact any of the organization's systems or infrastructure.

The backup imperative

When you do these things, you minimize the risk that attackers will breach your organization.

But here's the thing about attack prevention: It's never 100 percent effective. There are simply too many ways for threat actors to execute attacks, too many assets to defend and too many unknown risks to prevent every attack, every time.

One of your applications might be subject to a vulnerability that threat actors have discovered but that has not been publicly recorded, for example. Or, you might have overlooked some remote devices when mapping your attack surface, leaving them vulnerable. Or perhaps an employee falls victim to a clever phishing ruse, giving attackers access credentials to systems that are otherwise well-secured.

Due to these and thousands of other risks that you just can't reliably anticipate and mitigate proactively in every instance, relying on attack prevention alone to stop ransomware breaches is simply foolish. Indeed, the U.S. Cybersecurity and Infrastructure Security Agency estimates that only about 85 percent of cyberattacks could reasonably have been prevented ahead of time.[4]

That's why every business should assume that, sooner or later, it will face a successful ransomware breach. At that point, the difference between an existential business crisis and a mere disruption boils down to how well the business has protected its data – which is the topic we'll cover on the following pages.

[4] "Top 30 Targeted High Risk Vulnerabilities," CISA.gov.

DATA SECURITY

Part 1: Protecting Production Data

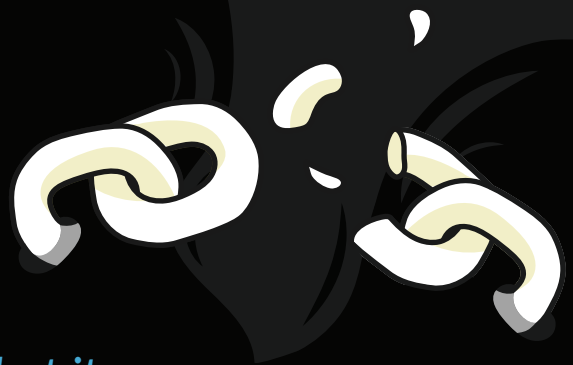
Mitigating the ransomware threat means protecting two main data types:

- Production data – the "live" data that IT systems produce and consume on an ongoing basis.
- Backup data – point-in-time copies of production data that can be used to recover data following accidental or malicious deletion or changes.

Let's start with production data

There are many steps organizations can take to protect production data.

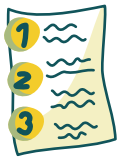
- Establishing strong physical security controls to prevent unauthorized access to the media that store production information.
- Investing in security awareness training to mitigate risks, like recognizing phishing/SMSishing, and not searching websites on company kit (some may be malicious), using removable media they've received or found, and sharing IDs and passwords.
- Keeping endpoints (like PCs and servers) up to date to protect against attacks that exploit software vulnerabilities.
- Installing intrusion-detection systems and antivirus software to detect active attacks.
- Backing up data so you can recover if it's damaged or deleted.



Let's dive deeper into what it takes to develop a backup strategy that keeps production data safe.

How to back up your production data

The following steps will ensure your production data and operations are as secure as possible:



Prioritize your data

Avoid the major expense of backing up all data, all the time by breaking your data assets into categories based on how business-critical they are, then defining backup strategies for them accordingly. For example, essential data should be backed up continuously to minimize the risk of loss. Data that's less of a business risk should also be backed up, but perhaps less frequently.

Define clear RTO and RPO goals

Recovering data is only effective if the backups are recent enough to support recovery needs. If you've added or changed business-critical data since your last backup, your backups are of little value. This is why it's important to develop a backup strategy based on two key criteria:

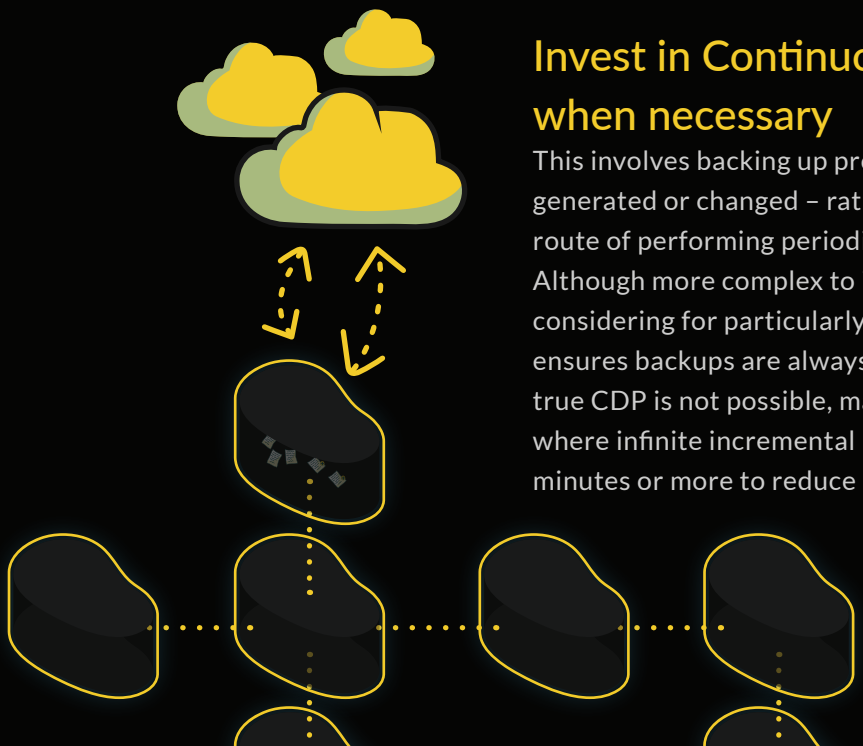
- Recovery Time Objective (RTO), the maximum downtime your business can tolerate through data loss.
- Recovery Point Objective (RPO), the biggest permanent data loss your business can survive.

The faster your RTO goals and shorter your RPO, the quicker you'll be able to recover lost production data and reduce risk of data loss/damage.

RTO and RPO needs vary for every business – even for different data types. For instance, data permanently lost from a documentation system can be recreated by your employees, whereas your ability to tolerate the loss of customer data is minimal.

Consider advanced protection techniques

For use with data subject to rigid RTO or RPO requirements, these include data mirroring (keeping two or more copies of your data available at all times to reduce the risk of data loss) and clustering (reducing the chances of data loss by spreading data across multiple storage nodes). Although complex and expensive to implement, they may be worth deploying for stringent RTO and RPO needs.



Invest in Continuous Data Protection when necessary

This involves backing up production data as soon as it's generated or changed – rather than taking the conventional route of performing periodic data backups or snapshots. Although more complex to implement, CDP is worth considering for particularly tight RPO requirements, as it ensures backups are always available for your data assets. If true CDP is not possible, many "near-CDP" solutions exist where infinite incremental backups are executed every few minutes or more to reduce risk of data loss.

Leverage instant restore technologies

This enables you to access backup data as if it's production data, so you can restore operations almost instantly following a breach. Many instant restore technologies are based on virtual machine (VM) backups that can be mounted to restore data accessed without having to recover the entire VM. Particularly valuable for tight RTO requirements.

Separate data assets

Segment production data into different databases, cloud storage services, object storage buckets and so on and establish access controls that require unique credentials for each storage resource. This reduces the risk of an attacker who breaches one part of your production environment holding all your data for ransom, stopping minor ransomware attacks turning into full-scale production breaches.

DATA SECURITY

Part 2: Protecting Backup Data

Why is backup data protection important?

Isn't the goal of ransomware to compromise production data, not backup systems? And aren't backups usually stored in a separate location, out of the reach of ransomware?

The answers, unfortunately, are "no" and "too often, not." While the primary target of most attacks is production data, in 93 percent of ransomware incidents, backups are compromised too.[5]

Ransomware attackers aren't dumb. They know if they can encrypt or delete your production AND backup data, you'll have virtually no choice but to pay the ransom, because you have no backup data to recover from.

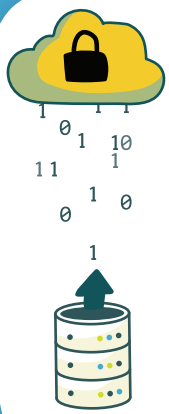
Meanwhile, storing backup data separately only works if you enforce rigid isolation between production and backup environments. Too often, ransomware attackers can use the same exploits to access production systems to break into your backups.

That's why taking deliberate steps to protect backup data is critical – it's simply your last line of defense against having to pay a ransom or suffer irreparable business damage.

Make backups immutable

This is the most important data protection technique for backups. It helps prevent tampering with backup data by hosting it on a read-only storage system, whether on-premises or in the cloud, so once data stored, it can't be modified or deleted.

Many backup solutions offer immutable backups regardless of the storage type, and most cloud service providers offer “object locking” to deliver immutability for backups stored on object storage in the cloud.



Encrypt backups

Obfuscating your backup data through encryption renders it obscure, unclear or unintelligible to attackers. This helps remove the threat of the disclosure of sensitive information, such customer social security numbers, that may exist inside compromised backups. It doesn’t prevent deletion, but does make it that much harder for the bad guys to breach your backups.

Adopt a 3-2-1 backup strategy

This involves storing THREE total copies of your data using at least TWO distinct storage systems, ONE of which is in a separate physical location from your production data.

Although this increases the complexity and cost of backups, as you have more storage repositories to manage and pay for, a 3-2-1 strategy makes it much harder for attackers to compromise all your backup data.

Consider air-gapped backup storage

Air-gapped backups are disconnected from the network. For instance, if you back up to tape media or removable drives and move them to an offsite facility, you have an air-gapped backup.

Yes, restoring takes longer because you have to reconnect your backup data to the network before you can begin recovery, but there is no way for attackers to compromise the data remotely. Unless they gain physical access to your backups, your backup data will remain intact.

Deploy anomaly detection

This scans backups prior to restoration to identify suspicious rare events, items, or observations that differ significantly from standard behaviors or patterns in the backup itself. It helps detect ransomware sitting dormant within your production data stores which could end up stored in your backups potentially re-infecting your production data when you perform a data restore. Some data protection solutions include a form of anomaly detection capability.

In short, data backup is the most important protection against ransomware because it’s the last layer of defense when all others fail. They are essentially your last hope for recovering data without having to pay a ransom.

[5]"Will data backups save you from ransomware? Think again." Security Intelligence.

THE ROLE OF CYBER INSURANCE

Before we close, let's touch on another topic that often arises in the context of ransomware and data protection. Cyber insurance is increasingly popular among businesses seeking to mitigate the impact of ransomware attacks, with the number of claims growing by 100 percent in the past three years. In fact, over a third (34 percent) of U.S. businesses have cyber insurance policies.[6]

And it's not hard to understand why. Policies pay out to soften the damages incurred through a ransomware attack. In that sense, cyber insurance provides another line of defense against ransomware risk.

No Guarantees

But sadly, like attack prevention, it's not enough to guarantee your business won't be severely harmed by ransomware. As payouts are typically limited, cyber insurance rarely fully compensates victims for the entire financial impact of an incident.[7]

Of course, getting some cash in the event you are attacked might soften the blow, but money won't give you back the years of data you might have lost. Nor will it restore your company's reputation if you suffer ongoing disruptions to your operations due to data loss, causing customers to question how much they can really trust your brand.

Reasonable Measures

On top of this, it's worth noting that in many cases, successful cyber insurance claims require businesses to prove they have reasonable protections in place simply to obtain coverage – and the more mature your protections, the less you're likely to have to pay for a policy. As the IT company Aldridge notes, "To qualify for cyber insurance, businesses must undergo security awareness training and testing."[8]

This means that if you can't demonstrate you've taken steps to protect your production and backup data, any cyber insurance coverage you've purchased might turn out to be worthless. Just as you can't expect your homeowner's insurance to pay out if you leave your doors unlocked, don't count on cyber insurance making your company whole if you suffered a breach after failing to protect your data.

[6]"64 Cyber Insurance Claims Statistics 2023-2024," Astra.
[7]"How Much Does Cyber Insurance Cost?" Embroker.
[8]"5 Requirements to Get Cyber Insurance in 2024," Aldridge.

TAKEAWAYS FOR MODERN RANSOMWARE DEFENSE

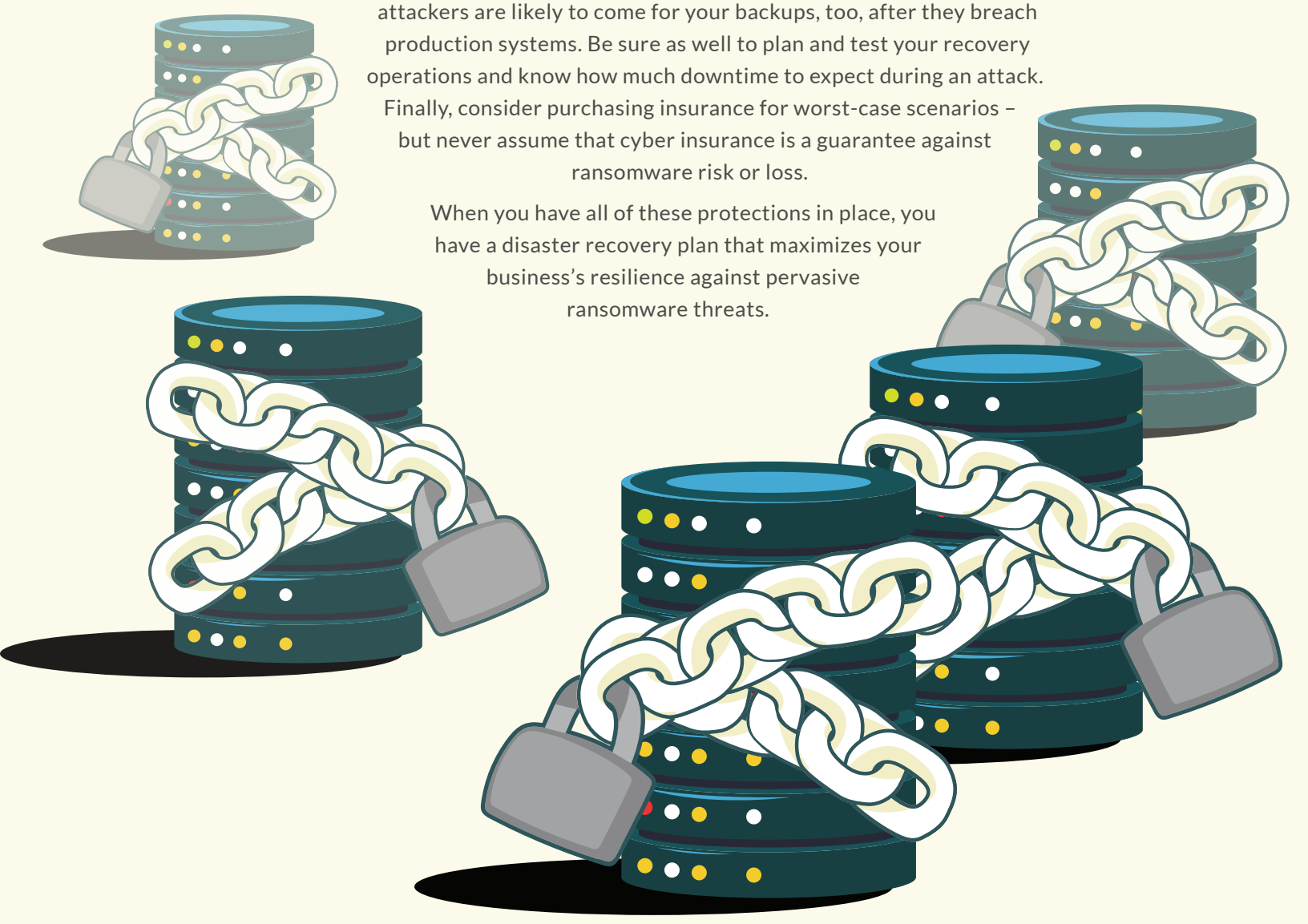
Guaranteeing that your business will never suffer a successful ransomware attack is simply impossible.

What is eminently possible, however, is investing in a multi-layered ransomware strategy – including not just technological defenses, but also practices like employee training and testing.

But even those defenses can be defeated, which is why performing recurring backups is the most important anti-ransomware practice of all. In the face of a successful attack, backups are the only way to restore business operations without paying threat actors.

To leverage backups to maximum effect, ensure that you protect backup data, since attackers are likely to come for your backups, too, after they breach production systems. Be sure as well to plan and test your recovery operations and know how much downtime to expect during an attack. Finally, consider purchasing insurance for worst-case scenarios – but never assume that cyber insurance is a guarantee against ransomware risk or loss.

When you have all of these protections in place, you have a disaster recovery plan that maximizes your business's resilience against pervasive ransomware threats.



Quest®

Quest® creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest solutions.

Quest NetVault® Plus provides comprehensive ransomware data protection and recovery that protects your production data and backup data, and ensures fast recovery after an attack. NetVault Plus delivers immutable backups, anomaly detection, encryption, object and cloud locking, air-gap backups, replication, continuous data protection (CDP), instant restore and more to combat ransomware and minimize business disruptions and data loss. Using NetVault Plus as part of a layered data protection and recovery strategy will greatly improve your ransomware resiliency.

For more information, visit: www.quest.com/products/netvault-plus