Winter is Coming: Are You Prepared for Disaster Recovery?

In the words of epic book and TV series *Game of Thrones*, "Winter is coming," and there's never been a better time to be on your guard. After all, we live in a world of vicious attacks, scary data breaches, unpredictable weather, and other factors that can threaten the very existence of both your applications and your precious data.

UNITRENDS

www.unitrends.com

Winter is Coming: Are You Prepared for Disaster Recovery?

Executive Summary

You don't have to strap on your armor and rev up your favorite clan vendettas to understand why the saga of *Game of Thrones* is relevant to disaster recovery. The series' beleaguered continent, Westeros, is much like a troubled enterprise—near-constant turmoil, management pressure and the continual threat of disaster. Like any enterprise or organization, Westeros is endangered by a lack of continuity and poor disaster recovery plans. The inhabitants of Westeros have much to teach anyone who's interested in business continuity and data recovery. This paper will explore why disaster recovery should become a priority for your enterprise—with the help of a few of the most memorable characters from *Game of Thrones*.

Why 'Game of Thrones'?

There's a reason *Game of Thrones* enjoys such incredible popularity. George R.R. Martin's bestselling series has sold millions of copies, readers are begging its author to hurry up and write the next book, and the HBO series based on the books has surpassed even The Sopranos as the network's most popular show ever. It's also uniquely suited to a discussion of the perils of an organization that hasn't put disaster recovery or business continuity front and center.

Think about it—like your business, Westeros is the center of all the action. Though your company may have seven (or 70) departments instead of seven troubled and conflicting kingdoms, it's likely that its history is as checkered and complex as the history of the Westerosi themselves. From The Stormlands to The Riverlands to Beyond the Wall, we wager that your enterprise faces just as many challenges as a tribe in *Game of Thrones*. And when you don't have a robust and well-tested disaster recovery or business continuity plan in place, you could be in for a conflict the size of the Battle of Blackwater.

Many of the ups and downs of the people of Westeros can be traced back to their reactive behavior in the face of personal and political disaster. While reactive choices and in-the-minute decision making makes for some great TV, your enterprise deserves better. When you make decisions from a place of fear or reactivity, you risk losing everything. Those split-second decisions could endanger everything you've worked so hard to build. Luckily, a well-constructed disaster recovery plan won't just make you look good—it can save time, money and even protect you from nightmare scenarios like expensive litigation and insurance exposure. It'll also leave you plenty of time to relax on the sofa with the latest episode of GoT.

Still think disaster recovery is an option instead of a must? Read on for some ways the characters from *Game of Thrones* can help you better prepare for disaster recovery and business continuity in your kingdom.

1. Survive System Overheating with Tyrion Lannister

Tyrion Lannister is one of the most loveable characters in *Game of Thrones*. He's a catalyst for wars and rebellions, a shrewd leader, and master of one of Westeros' most dangerous and mysterious substances—wildfire. A green liquid that cannot be extinguished by water, wildfire presents one of the biggest threats to the people of Westeros, causing massive damage wherever it is deployed and even threatening the capital city. Tyrion alone understands the damage the insane Mad King Aerys II Targaryen will inflict if he is allowed to unleash wildfire on his city, and Tyrion is the only one prepared to commit murder—even without credit—to prevent it from destroying everything.

Much like wildfire, data center overheating can literally destroy what you and your employees work so hard to produce. Outages, lost data, wasted time and energy, not to mention angry stakeholders and employees—what can't overheating ruin? Because it can be caused by anything from in-room dynamics to weather events, system overheating should be taken very seriously. It can wipe out your livelihood in one fell, hot swoop, burning up your reputation with it.

Data center overheating can even cause *Game of Thrones*-style outbursts that won't earn you any brownie points with your stakeholders. Take a tip from Tyrion Lannister and bow to the strength of overheating, then do something about it with a disaster recovery plan that focuses on both physical and virtual data.

Don't let a data center that's experiencing overheating due to inclement weather or in-center conditions threaten your livelihood. Ask yourself about your facility's vulnerability to overheating, and then make plans to back up and protect your data, replicating to a remote site (second site or cloud), for automatic failover and business continuity, no matter the thermometer reading.

Learn from Tyrion: You need a solid disaster recovery plan that can withstand wildfire—or at least data center overheating.

2. Survive Lost Talent with Ned Stark

Honorable but betrayed—what's not to love about Ned Stark? When Ned dares to challenge the man who succeeds his ill-fated best friend to the throne, he is betrayed, arrested and eventually executed, plunging the Seven Kingdoms into a brutal and shattering civil war. The sight of Ned's decapitated head on a spike when you tune into *Game of Thrones* isn't just great and gruesome TV, it's a lesson for anyone in danger of having their proverbial head chopped off when they lose talent.

Beware: lost talent could spur your own inter-enterprise war. Lost talent is just that—a loss, and one that could endanger your organization. Not only does lost talent present a threat to your data (think of disgruntled employees taking vital data with them), but any breach in continuity represents a real danger to your data. Where does it live? How is it managed? With the right business continuity solution, those questions won't complicate an already stressful employee departure.

Say goodbye to talent, not to your entire business. Ask yourself about the threats presented to your enterprise by lost talent, and then ensure that your organization is ready for incoming and outgoing talent. Also make sure your enterprise has planned for business continuity in its storage protocols and other procedures. You don't want the departure of one employee to threaten your entire institutional memory.

Learn from Ned: Survive the chop with your head intact. Be prepared for lost talent with a solution that keeps business continuity in mind.

3. Maximize System Resources with Davos Seaworth

Do you like your *Game of Thrones* with a stinky side of onions? Meet renowned smuggler Davos Seaworth. This lovable lowlife called on his smuggling background to get food—including onions—into Storm's End during a seemingly interminable siege. Sure, he had his fingers cut off for the privilege, but the Onion Knight is proud of his ability to spirit anything and everything into the right place at the right time.

Watch out—like Storm's End, your enterprise might have limited resources. We hope you're not under siege, but it can feel like it when you're stressing about how best to allocate and use system resources. When you're crunched for resources, every decision can feel like one that could result in having your fingers chopped off, and every decision can have real consequences across the enterprise.

That's why it's so important to have a reliable disaster recovery plan that focuses on making the most of your system resources. Your unwillingness to invest in a resource management plan now can have real—and very scary—ramifications in the future. Don't wait until you feel like you're under siege to figure out how best to manage system resources, even if it seems daunting.

Just because system resources are scarce doesn't mean you can't allocate them sensibly. Ask yourself about your biggest system resource allocation challenges, and then incorporate system resources into your disaster management plan. Consider investing time, energy and money into this vital part of your enterprise.

Learn from Davos: Incorporate system resource management into your disaster recovery plan.

4. Confront Targeted Attacks with Jaqen H'ghar

Jaqen isn't just any mystery man, he's a shapeshifter and a member of the mysterious guild of Faceless Men, a group of assassins who can change their faces at will. This enigmatic criminal is known for his assassin's talent as much as his strange demeanor. Don't mess with Jaqen—he definitely knows how to kill.

Is your organization being stalked by the shapeshifting assassin that is targeted attack vulnerability? A targeted attack can occur anytime and in any form. It can be almost maddening to determine when, where and how an attack may occur or if one has already occurred.

Worst of all, targeted attacks are just that—targeted directly to your organization. Talk about disturbing! If you want to sleep well at night (and secure your enterprise), you need a disaster recovery option that stays up-to-date on the dangers of targeted attacks and can protect you before, during and after an event.

A targeted attack on your organization can feel like just that: an attack. Don't be caught unaware. Ask yourself what you've already done to prevent targeted attacks, and then protect your system before, during and after an attack with a comprehensive recovery plan and frequent testing. You want to have the latest intelligence on targeted attacks and the proper tools to deal with them.

Learn from Jaqen: Targeted attacks can feel like shapeshifting assassins. Make sure your disaster recovery plan is agile and up-to-date enough to tackle attacks before, during and after they occur.

5. Face Untargeted Attacks with the White Walkers

Creeped out by Westeros' White Walkers? You're not alone. The inhabitants of the Seven Kingdoms had almost written them off as the stuff of fairy tales. Or at least, they did until the oh-so-eerie White Walkers emerged during a cold winter. These magical mummies can turn anything they touch into ice, reanimate the dead and only be killed when stabbed with dragonglass. Sure, they're not an immediate threat to most people, but they're still deadly—and plenty creepy.

Like the White Walkers, untargeted attacks can range from scary to deadly. Sure, they cast a wide net, but they still present a very real threat to your enterprise. If you're caught in the crosshairs of an untargeted attack, your organization can suffer just as much as it would at the hands of a directly targeted one. That is, unless you have the peace of mind of a disaster recovery plan that's current, flexible and powerful.

Don't get caught in the snares of a wide-scale attack. Ask yourself how an untargeted attack could threaten your enterprise, and then incorporate untargeted attacks into your disaster recovery plan with frequent testing and protocols that protect your system before, during and after a breach.

Learn from the White Walkers: Just say no to the creepy mummies of data. You don't have to fear untargeted attacks when your disaster recovery software is powerful, up-to-date and ready to roll.

6. Overcome Natural Disasters with Melisandre

The Red Woman Melisandre is a *Game of Thrones* fan favorite, and it's easy to see why. She's beautiful, mysterious, and has power over fire. And though her political predictions are sometimes off the mark and may come off as dire and dramatic, Melisandre embodies the raw, primal power of the elements, reminding us that "death by fire is the purest death." Sure, the scene where she gives birth to a deadly shadow is a bit over the top, but isn't that the privilege of being a mysterious priestess?

Melisandre's dark energy and erratic demeanor serve as a great reminder of the power and unpredictability of natural disasters. After all, we live in a world dominated by earth, air, water and yes, fire. Each of these can do irreparable and devastating damage when left unchecked. We've all heard of the tragedies suffered by enterprises that lose everything in a hurricane, flood, fire, tornado, or other natural disaster. While insurance money is nice, it can't make up for the manpower, hours, and sheer heart that go into your IT services, applications and data. Prepare your organization for the dark and often unpredictable energy of Mother Nature in all of her erratic glory with a disaster recovery plan that automates failover to a remote site shielding you from natural disasters while continuing operations.

Mother Nature is unpredictable. Ask yourself which disasters are most likely to affect your facilities. Give nature the respect it's due and ensure your data and applications are protected against floods, tornadoes, hurricanes, fires and other natural disasters.

Learn from Melisandre: Don't mess around with the dark forces of nature—incorporate the possibility of natural disasters into your recovery plan.

Summary: Is Your Disaster Recovery Plan Up to Snuff?

Disaster recovery shouldn't thrust your enterprise into an emergency on the scale of the Red Wedding. Be sure to pay attention to the following six factors when you make your plans for business continuity and disaster recovery:

- Data center overheating
- Lost talent
- System resource allocation
- Targeted attack vulnerability
- Untargeted attack vulnerability
- Natural disaster preparation

Winter Is Coming . . . Is Your Enterprise Ready?

Fess up—are you ready for a disaster? A siege? An attack? An assassin? (OK, we're hoping you don't have to deal with the last one, but you never know). If your answer is "no" or "I don't know" or even "kind of," you owe it to yourself to explore your continuity and disaster recovery options. Unitrends can help.

Here at Unitrends, we've earned our place at the forefront of today's disaster recovery industry through our commitment to engagement, experience and excellence. Simply put, Unitrends is the best cost-for-value provider in the IT protection and disaster industry, and we've got the awards—and the client list—to prove it.

At Unitrends, we know that your data and applications are at the heart of your business, your user experience and your worth as an organization. That's why we've created the industry's best cloud protection services, virtual appliances and hardware appliances to protect what you've worked so hard to build.

Isn't it time you took your seat on the throne? Earn your spot by doing disaster protection the right way. After all, you owe it to your company and your clients to anticipate disasters before they happen and make decisions before panic and reactivity—a la *Game of Thrones*—kicks in. Winter is coming, and now is the best time for business continuity and disaster planning. If your business—like Westeros—needs better protection, contact Unitrends to explore business continuity and disaster recovery options.