1105 MEDIA PAPER

Redmond MAGAZINE

CRITICAL EVENT RESPONSE: THE EXPANDING FOCUS OF IT RECOVERY PLANNING

backupify
a datto company

www.backupify.com

Based on a webcast featuring Jon Toigo, Chairman, Data Management Institute, and Ian Gillespie, Enterprise Sales Engineer, Backupify, a Datto company

Reports of cyberattacks and outages at cloud datacenters present IT organizations with a big problem that demands a solution. Loss of business-critical data because of a hack or a disaster (whether natural or manmade) can result in lost revenue, frustrated customers, and a damaged reputation. IT needs to be able to both secure data against hackers and restore data from a timely backup in the event of a ransomware attack as well as human error such as accidental deletion.

Moving IT infrastructure, apps and data to the cloud makes the need for a backup and recovery solution even more important. While cloud vendors are responsible for maintaining the cloud infrastructure and availability of applications such as the popular Office 365, IT is still responsible for the security and recoverability of corporate data. Cloud vendors have a good track record of not losing data (so far), but they do not protect against data that is deleted by malware or human error. If an employee inadvertently deletes an email that is later required for a legal proceeding, the cloud vendor is unlikely to help you hunt down that file and restore it.

"More and more companies are adding services and resources of public clouds to their on-premises computing," noted Jon Toigo, Chairman of the Data Management Institute. "This includes Software-as-a-Service offerings like Google G-suite or Office 365 from Microsoft. They are adding these externalized services to their own application sets even though they are hosted off-premise. These increasingly mission-critical workloads are often ignored when it comes to recovery plans. That creates a huge security gap in many cases."

Ian Gillespie, Enterprise Sales Engineer at Backupify, outlined the threat landscape IT is facing: "Ransomware is the big one. It's the most malicious of all the threats we see out there. There are so many variants and it's impossible to keep up with it. Ransomware is beginning to hit some SaaS applications—we'll only see more of SaaS-specific ransomware strains.

"It's also disgruntled employees, people deleting files and removing content. But it's not always malicious actions. With all of these new applications that we're flooding employees with, it's

Cover Image: Thanamat Somwan / Shutterstock.com

never been easier to access all of this data but it’s also never been easier to remove data or perhaps lose track of it because of the disparate number of tools.

“Finally, you have to take into account that as infallible as many of these cloud and application vendors claim to be, they all face downtime.”

Planning for ransomware and other potential human and natural disasters isn’t rocket science. IT knows the basics of what to do and what needs to be accomplished, Toigo noted.

”RANSOMWARE IS BEGINNING TO HIT SOME SAAS APPLICATIONS—WE’LL ONLY SEE MORE OF SAAS-SPECIFIC RANSOMWARE STRAINS.”

—IAN GILLESPIE, ENTERPRISE SALES ENGINEER, BACKUPIFY

“The fundamentals again, remain the same,” he said. “Disaster still equals an unplanned interruption in access to data for whatever constitutes an unacceptable period of time in your company. Secondly, the difference between an inconvenience and a disaster—between a crisis and a disaster—is typically measurable in terms of the duration of the interruption event itself. The longer it takes to regain access to a valid copy of data to drive your workloads and your decision-making, the worse the disaster becomes. The greater the length of time the disaster lasts, both tangible and intangible costs begin to add up.”

The key, of course, is having a disaster recovery plan and putting it into action.

“Smart planners develop capabilities that are designed to do two things, avoid preventable interruption events and recover quickly from interruption events that cannot completely be prevented,” Toigo said. “That is the mission of disaster recovery and the mission of IT recovery generally.”

COST OF DATA LOSS

Data loss, regardless of cause, comes with a hefty price tag. Given the potential costs, finding a great backup and recovery solution is always a good investment.

“To understand the cost,” Gillespie explained, “the average data breach costs $3.5 million. There’s a 27 percent chance that a US company will have a breach within two years costing up to $3.8 million. Last year ransomware cost the world $5 billion and that’s predicted to double in 2019 to $11.5 billion. That $5 billion isn’t just for paying the ransom: it includes business losses, and critical hardware that has to be replaced.”

Toigo urged IT departments to plan for the worst-case scenario and explain the dangers to the executives who may need to sign off on your plan. “I realize you may not have a hurricane or a tornado or a flood or any of these other weather disasters on a frequent basis, but when they do happen, they have a tendency to knock out not just the operations but the entire facility making things unavailable for a protracted period of time. Your plan really has to be structured in such a way that it deals with the worst-case scenario but it can be implemented in a modular way in response to the lesser emergencies."

> "SECURITY THREATS ARE INCREASINGLY A PART OF THE PANOPLY OF THREATS THAT RECOVERY PLANNERS NEED TO CONSIDER."
>
> —JON TOIGO, CHAIRMAN DATA MANAGEMENT INSTITUTE

CLOSING THE GAP BETWEEN DR AND INFOSEC

To protect your business from cyber-attacks and other threats to critical data, you need to tear down the wall between the folks planning disaster recovery, and those working on security. Among many things that they agreed on during a recent Fireside Chat, Toigo and Gillespie strongly recommended an integrated approach to DR and security. After all, if you can't recover your data after a natural or human disaster, you don't have anything to provide security for.

"Security threats are increasingly a part of the panoply of threats that recovery planners need to consider," said Toigo. "We've always had this distinction between the domains of disaster recovery and the domains of information security. Disaster recovery planning has been an activity that was separate and distinct from information security planning and they had different management, different skill sets, different missions and different budgets. And the two didn't work or play well together."

Disaster recovery was not usually given the status that security received, Toigo argued. "DR is often seen by business managers as just so much more insurance designed to satisfy auditors."

The only place disaster recovery touched in the security realm was in the area of data protection. Security came into the picture when data access became a requirement. Some still believe that backup still requires passwords, IDs, and possibly other credentialing from security, but this is an area that security and DR planning can agree that token access goes a long way to secure data.

The common security practice of keeping at least one copy of the data offsite is not safe unless the data is encrypted. Setting up encryption keys would include interfacing to the crypto security program. But that was about where involvement between security and DR ended.

Today, Toigo sees change on the horizon: "In an era of increased threats from hackers on the outside, disgruntled employees on the inside, we're all going to see the schism between DR and infosec begin to erode. We're going to need much more interaction and much more cooperation than simply on data protection and backup going forward."

NOT ROCKET SCIENCE

While technology, including virtual machines and the cloud, has changed the IT landscape significantly, the process of backing up still follows traditional guidelines, Toigo said. "We're still talking about doing the same three things we've always had to do when IT needed to recover from a disaster, which was an unplanned interruption event. Basically the three tasks of DR in a total meltdown are number one, recover your data to a usable form. Two, re-host your applications so you can operate again. Three, reconnect your users, which is both a combination to find a place for your users to work, getting them hooked up, getting the IP address systems working again so you can network over to the resources—whether they're in a recovery center or your original data center or in a cloud somewhere."

The important thing after any kind of disaster impacting IT is to get systems up and running as fast as possible. "Those three things have to be done and they have to be done in a timely way," Toigo said. "Some people refer to this as the recovery time objective. I call it 'time to data.' All these three things need to be accomplished in order to get back on a paying basis for your business. Those things haven't changed."

A BACKUP AND RECOVERY PLAN THAT JUST WORKS

Organizations are beginning to take note of the costs of data loss and many companies have already experienced damage first-hand, Gillespie noted. "One in three companies have already experienced data loss in SaaS applications. It is pretty shocking how many companies have reported data loss."

> "ONCE A WEEK, ONCE A DAY IS NOT SUFFICIENT. YOU NEED MULTIPLE BACKUPS PER DAY."
>
> —IAN GILLESPIE, ENTERPRISE SALES ENGINEER, BACKUPIFY

His advice to IT departments: "Prepare for the inevitable."

It starts with the almost obvious fact that you need to have a secure second copy of your business critical data, saved in a location that is different from where the data resides. "No SaaS provider offers that," Gillespie pointed out.

Microsoft's Service Level Agreement states multiple clauses that show they are not liable for data loss on the end user side. One such clause about app outages reads: "Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

For protection of data that may be needed beyond 30 or 90 days, companies need to have a plan for frequent and secure backups to a second location.

"Without that second copy, you truly are vulnerable," Gillespie said.

IT also needs to make sure the second copy has the latest data. Gillespie is an advocate for frequent backups: "Once a week, once a day is not sufficient. You need multiple backups per day."

FINDING A SOLUTION

Backupify has a checklist of what to look for in a backup solution:

- Automation
- Frequency
- Manual Controls
- Encryption & Security
- Retention

IT departments with tight budgets and limited human resources need to automate as much of the backup process as possible; an IT professional shouldn't have to spend valuable time doing routine and repetitive tasks. At the same time, you need manual controls so that you are in charge of the processes and can make needed adjustments.

Encryption is important for the security of the data. If you are going to store your backup data offsite in a physical location or even in a vendor's cloud, you need to be sure that data is encrypted to protect against hacking.

Read all the SLAs carefully, so you are sure the backup and recovery vendor is providing a comprehensive recovery and security system. It needs to make sure you retain older files for as long as business regulations and legal issues require.

Retention should be a consideration if your industry requires you to maintain data for a certain period of time. Ensure the solutions you consider are configurable and know what the limits of those features are.

CONCLUSION

No matter what stage of growth your company is in, SaaS backup should be an important part of your IT landscape. Be sure to test multiple disaster recovery scenarios, and backup solutions to fit your company's unique needs. The move to the cloud is accelerating, and the risk of SaaS data loss isn't a matter of "if" but "when."

Schedule time with our sales engineer for a one-on-one walkthrough of your business and how Backupify can protect you from the cost of downtime.

backupify.com/request-demo

backupify
a datto company