softchoice

6 Practices

for Better IT Resilience Planning

Introduction

As the quantity of data managed by IT organizations has surged, so too have the stakes in ensuring all of it is protected, secured and backed up. In 2013, IBM estimated that 90% of all digital data that had ever existed had been generated since 2011. The pace has only quickened since then, thanks to the ongoing uptake of cloud computing to support digital transformation initiatives, plus the proliferation of mobile devices and the emergence of the Internet of Things.[1]

IT resilience planning, which aims to ensure consistent system performance and protection despite any adverse events targeting sensitive data, is essential in this context. But taking care of such huge quantities of information can be challenging given the limitations of traditional backup technologies and the growing array of external and internal security threats.

Year-over-year, there has been a striking 56% rise in incidents and a 28.9% jump in affected records. Indeed, the question for organizations today is not whether, but when a breach will occur. How an organization responds, from getting key infrastructure back up and running to closing any vulnerabilities exploitable by insiders, will make all the difference.

A resilience strategy that combines modern measures for data protection and security is the best way forward. In this guide, we'll explore six best practices for better resilience, which collectively cover the key technical and procedural steps for improvement, including implementing Backup as a Service (BaaS) and eliminating operational silos that impede collaboration.

The Data Breach QuickView Report from Risk Based Security tracked 1,903 breaches in Q1 2019, involving **1.9 billion records.**[2]

1 www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/
2 pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Q1%20Data%20Breach%20QuickView%20Report.pdf

softchoice

Practice #1

Align Business Requirements and IT Service Delivery

It's common for business and IT personnel to be out of sync. A 2018 executive survey revealed that fewer than 40% of respondents felt that the two sides agreed on the role of IT and on the best use of technology across the organization. Furthermore, the survey found that business-IT alignment had degraded since 2012.[3]

This gap is most noticeable in areas like data protection, where there are often high expectations but no infrastructure in place to meet them. A recent Spiceworks survey found that almost one-quarter of organizations never test their backup plans.The main impediments were insufficient time, inadequate resources and a focus on other priorities.[4] With these constraints in place, critical systems may not perform as expected come crunch time.

In turn, the organization can suffer substantial damage to its finances and reputation. The problem in question could be a backup that takes too long to restore (or doesn't restore at all—a frequent problem with tape storage). A set of assets that couldn't be kept due to prohibitive costs but management assumed were still under maintenance.

Effective alignment between business and IT requires real accountability for specific projects and workloads, along with a shared set of budget priorities. Many IT departments exceed their budgets and, as such, would benefit from better tools and collaboration. The rise of practices such as DevOps demonstrate the potential benefits of removing silos. Meanwhile, cost-effective and reliable BaaS solutions make it much easier to achieve reliable, scalable backup.

3 www.cio.com/article/3307873/why-it-business-alignment-still-fails.html
4 community.spiceworks.com/blog/3138-data-snapshot-how-well-equipped-are-businesses-to-bounce-back-from-disaster

softchoice

Practice #2

Automate and Orchestrate Backups in a Unified Solution

In an ideal world, IT could manage all data protection workflows from one interface. Compared with the challenges of wrangling multiple systems, a unified setup offers a more dependable, more economical approach. Nonetheless, decentralized data protection solutions have been the norm.

By the end of 2016, over half of organizations were still maintaining two or more disparate solutions for data protection. Most of these relied on tape storage for data backup and archiving.[5] Moreover, 27% of them lacked complete insight into what was stored on these tapes. The predictable results were miscommunication issues and data/knowledge silos.

Relying on tape is time-consuming, to the point that organizations have the choice to invest significant resources in manual testing and other maintenance or opt not to test their backups. The latter leaves an organization with little to no understanding of how their backup and recovery solution might perform in a real crisis.

At the same time, the considerable cost in effort that goes into maintaining tape storage systems often outweighs the benefits. Tape often fails and many backups lack the setup for active monitoring and alerts. IT pays a steep price for this inefficiency, as they often lack the bandwidth to monitor everything by hand.

The best alternative to tape is a unified BaaS solution that can deliver:

- Dependable recovery of applications, systems or data at any time
- Orchestration and automation of testing and recovery workflows
- Full compliance with all applicable regulatory requirements
- Professional 24/7/365 management that reduces pressure on staff
- Improved resilience due to more thorough automation and reliability

[5] www.ontrack.com/resources/press/details/64993/survey-more-than-50-of-companies-run-multiple/

softchoice

Practice #3

Follow the 3-2-1 Rule and Move Beyond Tape

At some point, every tape drive will fail. Given the rising cost of data breaches and the growing spectrum of relevant threats, the risks of relying on this medium now far outweigh its benefits in terms of portability and familiarity.

Because tape is unreliable and difficult to maintain, it's wise to seek safer alternatives, such as a managed BaaS solution. BaaS enables organizations to diversify their backup and data protection strategies, automate numerous tasks and receive around-the-clock management from the service provider.

FOLLOW THE 3-2-1 RULE

It also makes it easier to adhere to the fundamental 3-2-1 rule, which advises:

3. Keeping at least **3 copies of important data**
2. Placing them on **2 or more different types of media**
1. Keeping **1 of them offsite for the sake of redundancy.**

The 3-2-1 rule has the official endorsement of several governmental bodies, including US-CERT.[6] In addition to helping its followers maintain multiple working backups, the rule also prioritizes moving beyond tape and toward more robust options such as cloud-based backup via BaaS, solid-state and hard disk drives and optical media.

A modern BaaS implementation might, for instance, place backups on an on-premises appliance and in the public cloud to comply with 3-2-1 recommendations and optimize overall IT resilience.

[6] www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

softchoice

Practice #4

Implement a Data Governance Strategy to Curb Risk

So far, we've focused on how to improve IT resilience through the lens of data protection, but security is just as essential. Implementing a data governance plan is a proven way to synthesize data protection and security requirements into a cohesive strategy. Governance can serve many purposes.

A given organization's approach to data governance might prioritize how information is stored, analyzed and accessed. It may also specify security controls and protocols. Effective governance is the linchpin of cybersecurity.

Having reliable, standardized processes and solutions in place makes it easier to defend against a broad spectrum of potential threats. From ransomware infections to dedicated denial-of-service (DDoS) attacks, there's no shortage of dangers that can precipitate a damaging breach.

In fact, **Trend Micro charted a 77% annual increase in ransomware attacks in Q1 2019** while also noting that some ransomware campaigns extorted millions of dollars from their victims.[7]

Staying resilient in the face of these challenges takes more than a modern backup strategy centered on BaaS. It also requires a governance plan that establishes shared security goals and priorities across departments and teams.

This, in turn, opens the door to more productive decision-making and increased operational agility. Well-implemented data governance promotes more regular and rigorous testing of applications, backups and critical systems for vulnerabilities. At the same time, proper data governance results in better stabilization of Agile and DevOps methodologies.

Because DevOps teams spin up new workloads and incremental updates at a rapid pace, data governance is essential for controlling any risks they might introduce in the process. Effective governance helps keep track of workloads, bring clarity to budgeting and ensure that backups are in place to guard against ransomware, In the case of ransomware, a solid data governance plan may be the only effective countermeasure.

[7] documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

Practice #5

Perform Continuous Monitoring

Continuous monitoring is integral to effective data governance, as this is the only way to determine whether current controls are sufficient and a given user's activities qualify as anomalous. Executed well, continuous monitoring will distinguish possible malicious behavior from normal workflows and flag unauthorized apps and files.

However, the scope and complexity of effective security monitoring is a burden for organizations with already-overextended IT teams. Specific challenges include gaining visibility into all of the necessary systems, setting proper baselines and dealing with human error from personnel performing repetitive manual tasks. Informational silos and blindspots are an inevitable result that increases the overall risk.

On the other hand, an automated approach to continuous monitoring will pay dividends. Specialized tools can gather analytics and inform recommendations for how certain controls (e.g. for access/authentication) can be adjusted as needed. Working with a managed service provider on security-related implementations can lead to more sustainable, scalable continuous monitoring that reduces silos and blindspots en route to boosting general IT resilience.

Practice #6

Create and Maintain an Incident Response Plan

It bears repeating that organizations must start from the assumption that they will be attacked and breached at some point. The Canadian Centre for Cyber Security has noted as much in its official guidance for baselining security controls and advises the creation of a detailed incident response plan.[8]

FOR THE PURPOSES OF IT RESILIENCE, SUCH A PLAN SHOULD AT A MINIMUM INCLUDE INFORMATION ON:

- Who is responsible for responding to security events, overseeing pivotal security systems and communicating with vendors and stakeholders.
- What external partners, if any, will assist during the recovery from an attack or breach.
- How long it will take to get critical systems back online, like in the wake of an unplanned downtown incident.
- The presence of any cyberinsurance policies that could provide financial protection for covered assets.

As a document, an incident response plan will piece together all of the best practices and steps for IT resilience discussed in this white paper, putting them into proper context and offering a clear way forward when an adverse event occurs. It establishes accountability throughout the organization, sets benchmarks for backup and offers insight into all of the security controls and mechanisms set up to guard against harm.

Having an easy-to-understand and widely shared plan simplifies incident response. Being prepared saves thousands or millions in otherwise avoidable costs incurred from a breach that wasn't recognized in time or responded to in concert.

[8] documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

softchoice

Power Digital Resilience with Data Protection and Security

Superior IT resilience planning requires consistent protection, security and data management. After all, data is the fulcrum of digital transformation. To succeed, an organization requires reliable backup and intelligent handling. Many solutions, including multicloud deployments and BaaS platforms, can ensure the necessary data protection and security along the way.

For example, a managed BaaS implementation places pivotal tasks, such as maintaining 3-2-1 backups and responding to outages, in the hands of a trusted service provider. The result is improved resilience for BaaS customers, who can then rechannel their resources toward more strategic projects without worrying about the integrity of their information. Data protection experts from Softchoice and Veeam have convened for an in-depth discussion of resilience planning.

This on-demand session covers the latest in enterprise data protection, backup and recovery planning, data-related outages and incident responses.

Get the details on our speakers and topics or view the full webinar.

Ready to move forward with IT resilience and data protection? Find out more about **Softchoice Backup as a Service** to protect your critical data and applications.

About Softchoice:

Softchoice is one of the largest IT solution and managed service providers in North America. Every day, thousands of organizations rely on Softchoice to provide insight and expertise that speeds the adoption of technology, while managing cost and risk.

Through our unique points of view, we challenge leaders to think differently about the impact of technology on their employees and customers.

Softchoice enables organizations to realize the full benefits of public cloud and a modern IT infrastructure through solution design, implementation, asset management, and assessment services, as well as ongoing support and mentorship through managed services.

With access to one of the most efficient and cost-effective technology supply chains in North America, Softchoice also ensures products get to our customers quickly and in a trouble-free way.

softchoice