softchoice

DIGITAL TRANSFORMATION:

Bridge the IT Resilience Gap

Digital Transformation: Bridge the IT Resilience Gap

The Digital Customer Experience: From Pilots to Scaling offerings

Success used to mean stability, at least in the business world. Back in 1965, an organization on the S&P 500 Index stayed on that list for 33 years, on average. Today, an organization's expected lifespan is a mere 10 years. Over on the Fortune 500, only 53 of the companies 1955 list have managed to avoid going bankrupt, being acquired or squandering their lofty market position.

This massive state of disruption isn't all bad news for enterprises. In fact, it represents a tremendous opportunity. Today, the playing field is level. All organizations have access to troves of data and the technology to do something with it such as cloud, artificial intelligence and automation. As such, enterprises across all industries have an opportunity to create new revenue models and – perhaps more important – innovative customer experiences.

$1.18 trillion

Global digital transformation spending to hit $1.18 trillion in 2019, an increase of 17.9% over 2018. - IDC[1]

[1] Worldwide Semiannual Digital Transformation Spending Guide, IDC

The IT Resilience Premium

What do we mean by IT resilience?

IT resilience is an organization's ability to maintain its critical processes and the IT systems that support them to acceptable service levels throughout severe disruptions.

The same elements that make disruption possible for all business – leveraging data and great customer experiences – are the same things that make it difficult. By relying on data and services coming in from the public or private cloud and expecting to access them at any time on any device, we make ourselves vulnerable. Assembling these elements in a way that won't let customers down and will result in unforgettable, uninterrupted experiences, can be daunting. But it's the reality we face. It's the IT Resilience Premium.

Today, IT must ensure the infrastructure and building blocks of modern applications are sustainable, functional and secure. And they must deliver "always-on" experiences and keep customers coming back, without losing their trust.

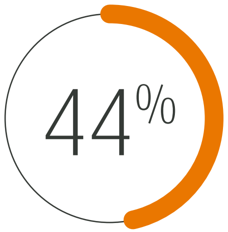
> "When your application crashes or fails to work as expected, you don't just lose time and money fixing the problem. You break the customer experience. And that costs you everything in our digital world."
>
> – Paul Dowling, Data Center Practice Lead, Softchoice

Why The Premium Is Worth Paying

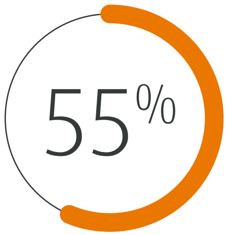
IT leaders understand that resilience is well worth paying for. In fact, it's one of the most crucial investments a digital business can make. Not only does the future of business depend on high-performance, always-on applications but so does the livelihood and happiness of customers.

This isn't hyperbole. Imagine a banking app, a fitness tracker, or a connected piece of machinery that tells a farmer when to harvest his crops. When an application becomes part of your customers day-to-day life – or livelihood – a poor experience can impact your brand reputation.

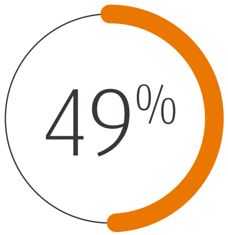
What IT leaders fear about poor application user experience:



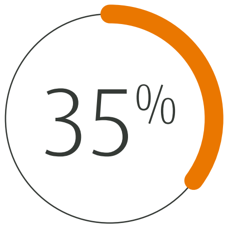
Say it poses a threat to the existence of their business



Say it prevents delivery of a good customer experience



Say it will result in lost revenue



Say it will result in a direct impact to customer livelihood[2]

[2] 2019-20 Global CIO Report, Dynatrace

The IT Resilience Gap

Just because it's critical, doesn't mean it's happening.

In fact, a recent study shows most businesses are unable live up to the IT Resilience Premium. The gap is wide:

- 73% of businesses are unable to meet user demands for uninterrupted access to applications and data
- Enterprises experienced 5 to 10 unplanned outages in the last year
- Only 37% believe they can reliably back up and recover within target SLAs[3]

So, why the gap?

From not having the tools to identify performance issues, or the processes in place to get back online in the event of an emergency, there are four key areas that can make or break an IT Resilience strategy:

1. Limited application and user experience insights
2. Outdated recovery approaches
3. DevOps pitfalls
4. Cybersecurity resilience

[3] Cloud Data Management Report 2019, Veeam

1 | Limited Application and User Experience Insights

If you can't measure it, you can't manage it. But this is exactly what happens as enterprises adopt a wave of new applications, platforms and services delivered through the cloud, but fail to scale up or widen their ability to monitor those new workloads.

Today, traditional monitoring of the three-tiered infrastructure is still relevant – but to maintain performance and identify issues, IT requires insights, on the application layer. If you can't tell how well your application is working, from a user experience perspective, you will have a hard time fixing and preventing long, drawn-out outages, delays and negative user experiences.

76% of CIOs say they don't have complete visibility into application performance in the cloud.[4]

THE KEY REASONS IT LACKS PERFORMANCE INSIGHT:

User experience metrics: IT finds out about performance problems from end users 70 percent of the time, according to Gartner. This is already too late. IT must be able to spot user issues and find fixes before they become a problem. To do so, they need to establish, track and improve key performance indicators from the user perspective (such as page load times), as well as more traditional systems and availability factors.

Root cause analysis: Legacy performance monitoring tools worked fine on "monolithic" applications, but modern apps are often scattered across numerous environments and layered across multiple different functions, such as with microservices. Without a unified, real time window into the entire application footprint, IT cannot hope to track down issues and avoid delays. In fact, with siloed, domain-specific tools, it often takes days—if not weeks—to isolate and fix performance problems

Application dependencies: When a business migrates a workload or updates its applications and infrastructure, it's not easy to predict the full impact it will have on performance. Until IT can see and understand every one of the connections and application dependencies in the environment, including databases and external services, it will be unable to reduce the possibility of missing key dependencies during the move. But this step is essential for preventing unnecessary downtimes, outages and hiccups.

[4] 2019-20 Global CIO Report, Dynatrace

2 | Outdated Recovery Approaches

In the event of an emergency, the ability to get back online fast and reliably is critical. You can't always avoid disaster. So, when strikes, your backup and recovery plan is your best hope at preventing a terrible situation from devolving into a catastrophe. Today, however, IT leaders are struggling in this crucial area.

According to Veeam, **69% of businesses have lack the capacity to recover applications at the speed expected of an always-on enterprise.** Moreover, only 37% are very confident that virtual machines can be recovered within the Service Level Agreement. As a result, businesses are parting with upwards of $20 million a year in lost revenue due to application downtimes.[5]

WHY IS THIS HAPPENING?

No automation: Many IT organizations still depend on manual, case-by-case responses when a key resource goes offline. This not only costs precious time but the pressure to recover fast also creates additional exposure to configuration errors.

No standardization: When every workload, across every environment, is architected using a different approach and managed by a different team, mistakes flourish. Delays ensue. Organizations must wrestle with legacy tiers and silos to improve the team's capacity to respond to an event, across the entire application stack.

Need for intelligence: Almost all businesses (98%) are looking to artificial intelligence, big data analytics and other emerging technologies to add more intelligence to their data management arsenal, according to Veeam. But until those plans are realized, they will continue to face the consequences of slow, ineffective capabilities in managing, backing up and recovering critical data.

[5] Cloud Data Management Report 2019, Veeam

3 | DevOps Pitfalls

For most enterprises looking to disrupt rather than be disrupted, the path forward will call for more than new customer experiences. Innovation also requires new ways to create the software driving those experiences. This is the reason DevOps is so critical for the creation of successful, resilient modern applications. However, as more organizations adopt DevOps several challenges begin to appear. And when DevOps projects fail to mature, applications are slow to evolve, customer expectations are broken and, very often, security is put at risk.

WHY DEVOPS STRATEGIES FAIL:

No security alignment: According to a recent survey, only 14% of organizations had integrated security across the entire DevOps lifecycle, including requirements, design, building, testing, and deployment. While DevOps helps a business move faster, failing to align it with security at every step leaves the door open to breaches. The results? Data loss and severe damage to brand reputation. The DevSecOps model assumes everyone is responsible for security.[6]

Slow adoption: Another survey of more than 2,000 IT industry executives in the midst of adopting DevOps found that 54% of respondents said they had no access to self-service infrastructure. Only 23% said infrastructure could be delivered in less than 24 hours, while 33 percent said it takes up to a month to do so. Some 26% said it takes one month or more.[7]

Rogue users: The same study shows a general lack of central governance and automation when it comes to creating new application environments. This leads to pockets of developers using their favorite, often not well-integrated, DevOps tools.

[6] State of DevOps Report, Puppet

[7] Top 10 Challenges to DevOps Implementation, Tech Republic

4 | Resilient Cybersecurity

Cyberattacks are one of the biggest and most expensive threats to IT resilience. Not only are the stakes getting higher, with the average cost of cybercrime increasing to $1.4 million, they are getting more sophisticated doing greater damage to the customer experience.[8]

Take ransomware attacks, which are on the rise for enterprises, with a 500% increase year-over-year.[9] As cyberthreats increase in scale and frequency, IT must overcome in order to enable new business growth and reliable customer experiences. In fact,75% of businesses say downtime is the costliest part of a cyberattack.[10]

TOP CYBERSECURITY CHALLENGES:

Staying on top of threats: A whopping 99% of vulnerabilities exploited in 2020 will be ones known about by outside security and IT professionals for at least one year. Meanwhile, as the window of vulnerability grows in step with the severity of the threat, making manual threat prevention and remediation much more difficult.

Skills gaps and limitations: There will be 3.5 million unfilled cyber security positions , making it next to impossible for companies to keep pace with the dramatic rise in cybercrime. Today, say skills shortages are impacting security operations.[11]

Human error: Organizations are split on whether the most dangerous cyber threats originate from malicious outsiders or those inside the enterprise. According to a Kaspersky Lab report, more than 46% of cybersecurity incidents result from human error.[12] To overcome our natural shortfalls, IT must find automated, intelligent ways to mediate access to the right data, at the right time, to the right person.

Incident response: When a breach occurs, IT must have the ability to mount a fast, effective response. Yet, 25%of cloud security alerts go unaddressed and more than half of enterprises admit they can't keep up with security incidents. Moreover, 83% feel they do not have processes in place to be effective in acting on security incidents.[13] Talent shortages, budget challenges and lack of practice all share the blame for lack of incident response readiness.

[8] Ninth Annual Cost of Cybercrime Study, Accenture
[9] The Top Cyber Security Trends in 2019 (and What to Expect in 2020), The SSL Store
[10] By the Numbers: Global Cyber Risk Perception Survey, Marsh
[11] The Top Cyber Security Trends in 2019 (and What to Expect in 2020), The SSL Store
[12] Balancing future opportunities with future risks: A global survey into attitudes and opinions on IT security, Kaspersky Lab
[13] PERSPECTIVE: Government Agencies Must Adapt to New Reality of Cloud Threats, Homeland Security Today

○○○○○○○○●

Conclusion

The prize of digital disruption is there for the taking. If your business can assemble a unique and powerful way to leverage data, drive new revenue models, and engage customers, almost nothing can stop you. Almost nothing.

Of course, there is application performance to worry about. And downtimes. And letting your customer data fall into the wrong hands or getting smacked by ransomware.

That may sound daunting, but there are a series of proven solutions and best practices which can help you overcome the gaps and deliver sustainable digital success.

▶ To learn about those, check out **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.