EMPYREAN

Ensuring Certainty in Uncertain Times

3 Mobility Must-Haves for Ben Admin Business Continuity

INTRODUCTION

COVID-19 has challenged businesses everywhere to adapt to a new way of working. Nearly every aspect of business has become virtualized, including the business of human resources and employee benefits. Mobility, data integrity and security, and compliance are more crucial than ever in today's virtual world – and there's less room for errors than ever before. This is particularly apparent when it comes to your employee benefits administration.

Employees and their families are relying on the benefits you provide to keep them prepared and protected throughout this global health crisis. While some organizations are still grappling with the new operational demands of the pandemic, your benefits administration provider is one the vendor you should never have to worry about.

This At-A-Glance will guide you through three key factors when evaluating the preparedness, crisis response, and long-term stability of your ben admin vendor. With the right partner in place, you and your employees can be confident that you're always supported, no matter what may come next.

1 | Strong Mobility Strategy

The COVID-19 pandemic has highlighted the necessity of having a robust mobility strategy like never before. Practically overnight, organizations that had previously hesitated to adopt telework capabilities were suddenly forced to support a fully remote workforce.

As a result, many companies are still struggling to bring their now virtual operations up to speed. Even those businesses that embraced occasional telework have grappled with the unforeseen challenges of expanding capabilities for daily use across their entire team.

The way you work may have permanently shifted, but the reliability of your outsourcing partners should never be impacted – regardless of the challenges facing your own organization. While many vendors claim to have a business continuity strategy, not all have incorporated mobility as a central part of that strategy.

A strong mobility strategy will enable an entire organization to continue running at full capacity from *any location* – securely – and for any length of time. This ensures that your benefit services will continue uninterrupted through local, nationwide, or global disasters. The priority when developing such a strategy is to stay prepared for the unexpected, even those as unforeseen and far-reaching as a worldwide pandemic.

Digital benefits access is especially crucial to the success of both your HR team and your employees. Leveraging an online benefits platform allows you to manage your benefits strategy outside of the office, and enables your employees to enroll and engage with their benefits from virtually anywhere.

"Over one-fifth of employee visits to the Empyrean Platform are made on a tablet, smartphone, or other mobile device."

And with 96% of Americans now owning a smartphone[1], mobile benefits applications such as EmpyreanGO℠ and Empyrean Pilot+℠ offer a familiar and easy way to keep your benefits top of mind when outside of the office.

For a function as critical as employee benefits, your outsourcing provider's services cannot be bound to any one physical location. Your provider should not require a central facility to stay operational. However, a mobility strategy is not limited to enabling remote work alone. It must also extend to your vendor's technology infrastructure, as well as how data is housed, accessed, and protected.

As many organizations have already experienced, implementing mobile capabilities is not as easy as flipping a switch. Instead, it requires expert consideration, execution, and continuous maintenance to ensure plans are ready to deploy at a moment's notice.

Key Questions to Consider

1. Did your benefits administration provider incorporate mobility as part of their business continuity planning *prior* to COVID-19?

2. How did your partner demonstrate their mobility strategy at the onset of COVID-19? Did the experience match your expectations?

3. Has your partner clearly communicated the steps being taken to ensure your service remains interrupted?

4. Has your solution or service quality been negatively impacted by the pandemic (or another natural disaster) in any way?

5. Given your experience, are you confident that your benefits administration provider will be ready to tackle an unexpected crisis in the future?

2 | Smart Investments

While current events have made clear the advantages of having a reliable mobility strategy, there are a number of reasons why some companies have traditionally hesitated to implement their own.

For some organizations, focusing on mobility requires a mindset shift that had previously been difficult to overcome. For decades, there have been misconceptions surrounding the productivity and professionalism of remote employees.

This perspective was tough for more traditional employers to change. However, 44% of employers have actually reported an increase in employee productivity after the pandemic-driven shift to remote work.[2]

83% of employees want the freedom to work from home at least once per week and over half of executives (55%) plan to incorporate a work-from-home policy even after the threat of COVID-19 has passed.[2] With so many employees displaced from the office, employers and employees everywhere are discovering the mutual benefits of remote work – so the practice is likely to here to stay.

As mentioned previously, however, a robust mobility strategy goes beyond occasional remote work capabilities. **A truly proactive strategy must be scalable and extend to your benefit partner's *entire* organization – including their operations, technology, and customer service teams.**

Developing a mobility strategy is only the beginning. **It takes significant *and continuous* investments to ensure a successful execution.**

In order to fully implement their business continuity planning, your partner has to consider every detail of their business and operational processes. This includes how their team is structured and dispersed nationwide, their data storage and security, and even the stability and preparedness of their own vendor relationships.

2 | Smart Investments
continued

One particularly important element in this equation is the **hardware** your partner chooses to use. Having a mobility strategy means staying *mobile* – **so it is crucial that your benefits provider utilizes *mobile hardware* across their entire organization.**

While desktop computers are less expensive to purchase and replace, they are also bulky and office-bound. The use of desktop computers poses a major business continuity risk if an office becomes inaccessible.

To eliminate this risk, your outsourcing partner should utilize laptop computers for every team member. While this solution may seem simple enough, this change requires an investment that can be anywhere from *two to three times greater* than the cost of traditional desktop computers.

Along with this hardware, **your provider must also utilize a virtual private network (VPN) to allow their team to work securely while outside of the office, and protect your sensitive data at all times.** Every member of their organization should be able to access this VPN *simultaneously* – which in itself requires the right setup, testing, and supervision to maintain.

Key investments in your partner's technology will ensure all of your services continue running smoothly. A strong provider will have also made smart investments in their business to support their team, prevent the need for downsizing in a crisis, and keep service quality high in any situation.

Key Questions to Consider

1. What investments has your benefits administration provider made as part of their business continuity planning?

2. Where are your outsourcing partner's offices located? Are offices and teams spread out across a large area, or centralized in one location?

3. How has your benefits partner prepared in the event that their offices are inaccessible?

4. Does your partner utilize mobile hardware and a VPN across their *entire* organization? Were these measures in place prior to the COVID-19 crisis, or were they only recently implemented?

5. Has your outsourcing provider experienced downsizing or layoffs due to the pandemic? If so, how has this impacted the service quality that you and your employees receive?

6. Does your partner have the proven history and secure financial backing to ensure continued service over the long-term?

3 | Data Management & Security

In today's virtual world, data security is more important than ever. Without the right safeguards, your data – *and your employees' most sensitive information* – can be put at risk and fall into the wrong hands. Conversely, this data must also remain accessible by your team and authorized parties in order to keep your employees protected and your benefits strategy on track.

How your benefits administration outsourcing partner handles your data, manages data transparency, and ensures data security is a major factor in the success of their mobility strategy, overall disaster planning, and your solution's long-term stability.

Many vendors say they store their data "in the cloud" – but what exactly does this mean? How safe is your data when *and where* it's stored? What redundancies and backups are in place to keep you protected?

With a physical storage location, your valuables are only as safe, secure, and accessible as the facility where they are stored. The same is true of your virtual data storage. **If your benefits administration outsourcing provider utilizes a third-party cloud, your solution is only as reliable as their cloud vendor's security and continuity measures.** If their third-party vendor fails, so will your solution.

A best-in-class benefits administration provider will eliminate third-party risks by owning and managing their *own* cloud system.

> ***"A business-critical solution demands reliability and availability across its entire infrastructure, including the cloud behind the scenes. A private cloud approach is the best practice to minimize dependency on third party public cloud providers. It ensures a dedicated focus on the systems that support your solution, to keep them running smoothly and securely – no matter what."***
>
> **- Rick Miller**
> **VP Enterprise Technical Services, Empyrean**

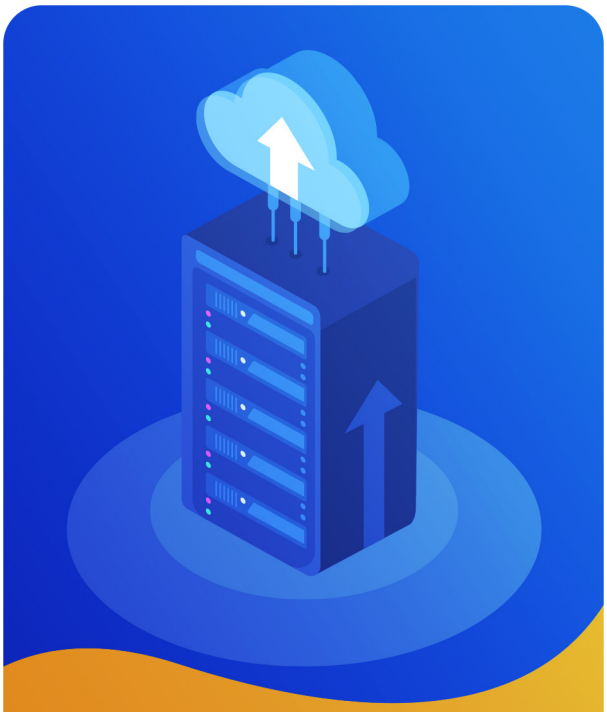
Keep in mind, however, that **only 1% of enterprise organizations leverage this kind of private cloud approach.**[3] A private cloud ensures that your outsourcing solution will not be subject to the failures or data breaches of another vendor, and also allows for better scalability, enhanced security measures, and optimal handling of traffic on the system. There must also be multiple redundancies in place with defined recovery times, to keep your benefits data accessible in the event that one of their data centers experiences a failure.

3 | Data Management & Security
continued

Another key aspect to look at when evaluating your partner's approach is the way they house each client's data. **Specifically, your chosen system should utilize a *single-tenant architecture*, where your data is housed separately from other clients on the platform.** This allows for faster, more customizable and accurate configuration, more robust testing functionalities and error prevention, and an overall more secure and reliable solution.

The alternative to single-tenancy is *multi-tenancy*, an operationally lower-cost option where all client solutions and data co-exist on a single instance of the platform. A multi-tenancy approach is less expensive for your vendor to maintain, but it will leave you with fewer customization options, longer configuration periods, and open to testing, accuracy, and security issues.

And while a vendor may say that your data is encrypted, not all methods of encryption are equal. Only 1% of enterprise organizations leverage a private cloud approach[3]



Only **1%** of enterprise organizations leverage a private cloud approach

"Flexera 2020 State of the Cloud Report." Flexera. Itasca, IL. April 2020.

3 | Data Management & Security
continued

Basic disk-level encryption only protects your data from access when the disk it is stored on is not spinning (in use). This type of encryption is less costly for a vendor, but leaves their client open to major security risks and makes redundancy difficult.

In contrast, **bit-level encryption ensures that your data is always encrypted –both when in use and at rest – and makes redundancy easier to achieve.** This advanced level of encryption requires a significant investment on the part of your provider, but a best-in-class partner will have already made this a key element of their data security methods.

Beyond this, every click within your platform must be tracked and monitored by user, and continuous patching should be prioritized to ensure their system is always up-to-date.

Given the importance of the data being managed by your benefits administrator, the minimum standards are simply not enough. Take time to thoroughly vet and understand the processes, safeguards, and tools your benefits partner is using to keep your data accurate and secure.

How does your partner's security measures stack up – not only against similar providers, but also among other data management and security-focused organizations? What best practices has your partner adopted that not only meet, but *exceed*, industry standards?

If not properly managed, your benefits solution can face critical threats, including everything from natural disasters to hacking exploits. How your benefits administration partner approaches data management and data security will make a significant difference in your solution quality, employee satisfaction, and peace of mind.

Key Questions to Consider

1. How and *where* is your benefits data being housed? What redundancies and processes are in place to ensure your data will remain accessible? In the event of a major disaster, what is the expected recovery time to have your solution back up and running?

2. What level of encryption does your partner utilize? Is your data continuously being protected both when data is being accessed as well as at rest?

3. How does your vendor's data management and security methods compare to industry best practices and other leading organizations?

4. Does your organization own and manage their own cloud system, or are they reliant on a third-party cloud service?

5. Does your system utilize a single-tenant architecture, or a riskier multi-tenant approach?

6. To what level is user activity tracked across the platform?

Conclusion

The sudden emergence of the coronavirus pandemic has demonstrated the requirement for strong business continuity planning. It's crucial that you closely examine and evaluate the preparedness level of your vendor partners, especially when it comes to managing your employee benefits.

Gaining a more thorough understanding of these processes will help you clearly evaluate a potential partner and know what you should expect during an emergency as well as day-to-day.

Without a reliable and well-prepared partner, even the most thorough plans can fail. However, with the proper support and planning in place, you can deliver certainty for your employees, their families, and your business – even during the most uncertain times.

References

1. "Mobile Fact Sheet." Pew Research Center. Washington, DC. June 2019. *https://www.pewresearch.org/internet/fact-sheet/mobile/*
2. "When Everyone can Work from Home, What's the Office For?" PwC. New York, NY. June 25, 2020. *https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html*
3. "Flexera 2020 State of the Cloud Report." Flexera. Itasca, IL. April 2020. *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*