

7 REASONS TO INSTALL YOUR OWN HR SYSTEM AND AVOID CLOUD DEPENDENCE.

7 REASONS TO INSTALL YOUR OWN HR SYSTEM AND AVOID CLOUD DEPENDENCE.

The best reasons not to trust your important data in the cloud. Including cost, management, security, data protection and your business needs. 8 mins reading time

COST OF USE

Cloud based software sounds great. But, the cloud is mostly just great for the vendor. Startups and fast-growing firms can build infrastructure in the cloud quickly. Cloud based software can easily scale in ways that would be hard to achieve quickly any other way. If you are in the business of writing software you can install it on very large server farms and support lots of different customers. Adding more and more customers is simple once you have written the code. You might think that this is going to keep the prices down for customers who pay to use the software. The fact is that cost reduction is something that the vendors all tend to emphasise. But it is not actually true. Most businesses find that the cloud is not as cheap – or even as flexible – as was claimed. Cloud does not save money, but it has been historically perceived and marketed as cheaper. Although cloud computing comes with low Capital Expenditure costs, there is a perpetual ongoing monthly fee. Most businesses spend considerably more cash on the cloud's life-cycle subscription. Also, the baseline standard cost can exclude a lot of functionality, which can quickly add up.

MIGRATION COSTS

The cost of migrating your existing data to cloud based software should not be underestimated. To cost of migrating back out when you want to leave can be even more. It is not unusual for cloud providers to have penalty clauses making leaving painful. Organizations often migrate gradually rather than switching instantly. This approach reduces operational risk and allows systems to be adapted step by step. This means you are still paying monthly paying cloud fees during the migration process. If your software is on-premise the migration cost is kept minimal.

VENDOR TIE IN

Terms of service can and do change at will. Cloud companies reserve the right to change these words at any time. This is not OK in our personal relationships, nor is it acceptable in business. If you sign a mortgage document the contract is a contract. The same is true when you lease something or any other transaction. This expectation goes away with provided software. The

end-user license agreements that come with most applications, and the terms of services required for any on-line service, aren't static. They can change at the provider's whim. What happens when a cloud provider goes out of business or is taken over? Generally there are negative consequences for you, the customer. Will your data continue to be stored with the same diligence, care and conditions that you originally expected? If they go out of business will it even be stored at all?

Furthermore, the more you become dependent on the cloud vendor the harder it is to extricate yourself.

Our software "HRCompleteManager" is installed on your own premises. Like all on-premise solutions You own the copy of the software you have bought. It is installed on your own computer and under your control. Once installed, there is no annual costs. It is yours to use in perpetuity. If you choose to pay for annual support and upgrades you can. But you do not have to and the software will carry on working on your PC. The cost of this ownership is generally comparable to less than one years fees for cloud base software.

DATA PROTECTION, COMPLIANCE AND SECURITY

It has to be said that cloud providers have invested heavily in security over the past decade. Frankly, they needed to. Their size and scale allows them to attract talented developers and employ sophisticated security tools. Cloud providers cannot afford to be victims of hackers and other cyber attackers. That said, there is barely a week goes by when a large scale attack occurs on some cloud software or another. Often it is extremely disruptive and the costs are eye watering. In 2025 alone I can remember:

1. Attackers grabbing data from the sales management giant Salesforce in at least two breaches.
2. The ransomware group "Clop" exploiting a vulnerability in Oracle's E-Business internal which they exploited to steal data from hospitals, health care groups, media companies, universities and The Washington Post.
3. Other affected businesses included Cloudflare, DocuSign, Verizon, Car Gurus, Cisco, LinkedIn, Nike, The Co-op, GitLab, SonicWall, Adidas, Louis Vuitton, Chanel and Transunion.
4. Jaguar Landrover stopped production for months and admitted to losing up to £50 million (\$70 million) per week.

The simple fact is that the resilience and security claimed by the cloud is for their infrastructure as a whole. They sometimes provide little protection – for a customer's data at file level. Not having control over your company's security is a considerable risk. Although vendors appear competent with the security of their platforms, it is your decision whether to trust them with your most sensitive data.

Furthermore, You still have to invest time and money in backup, recovery and local data protection.

ENVIRONMENTS, SPEED AND LATENCY

Access to cloud based system requires internet connectivity. Whereas on-Premise systems can operate in isolated networks or completely offline environments, including closed corporate infrastructures and air-gapped systems. Guess which one is more secure by design? Also, cloud speed and latency depends on internet connectivity and remote server response time. For on-premise system, performance depends only on local hardware and internal network. Guess which one is faster by design?

DATA RECOVERY

What happens when something goes wrong? With the cloud access to vital information is impossible if the internet connection fails. Or the vendors servers fail. Or any of the routers that relay your information between you, your ISP and the vendor. Data recovery is a time-consuming process for the system since businesses don't have instant access to their equipment or data.

With on-premise solutions like HRCompleteManager your software and database are stored on computers you control on your own premises. You can take automated backups, hourly, daily or as frequently as you choose. Should you ever need to, restoring data from yesterday, last week or an hour ago is simplicity itself.

SOVEREIGNTY

One important factor that many people overlook is where your data is stored. Sovereignty is a big issue in data protection. Laws and regulations, geopolitical events and foreign business practices affect your data. It is not only healthcare and finance that this affects. Your data has to comply with your laws and the best way to do that is to store it under your control on your own site.

WE HAVE BEEN HERE BEFORE

Cloud computing is based on the time-sharing model that made companies like IBM wealthy years ago, before we could afford our own computers. Then along came the personal computers that businesses could afford. Computers like PC's and Macintosh. This enabled businesses to take control of their own data. The business model of the cloud is the same as time-sharing.

The image in this article is © Jose Nicdao <https://www.flickr.com/photos/jonicdao/3450233884>

Thank You Jose for letting us use your lovely photograph.

Thank you for downloading this article. We have other articles on our website. Plus White Papers, Policies, Forms and Utilities that are free for you to download.

Reduce your manual admin and paperwork. Centralise your employee data and processes and reduce your compliance risks and legal stress. Reduce the time spent in managing employee data and free up time to concentrate on strategy, growth and profit.

HR Complete Manager is available in 3 different license bundles: Owner/Manager, Growing Teams and Corporate versions. There is a version to suit all businesses

HRCompleteManager.com