BIZCOMMUNITY

# Making data management do the 'heavy lifting' for the construction industry

Despite hopes of a turnaround, the construction sector remains in the doldrums. Its contribution to GDP contracted slightly in 2019, continuing a slide that has been happening since 2017. The picture isn't likely to change soon and, as a result, architecture, engineering and construction (AEC) companies are 'building in' business optimisation to ensure continuation.

By Chris de Bruyn 23 Jan 2020

Image source: Gallo/Getty

Myopic mindsets have unfortunately led many to neglect managing their data. There still remain traditional views in the industry that data is not a vital component to operations. Yet AEC is a very data-dependent sector. Sharing accurate information and establishing a ‘single truth’ are crucial for timely delivery and healthier margins.

## Data: Blueprint for profitable construction

Such measures have become even more important in the current market. The costs of materials are steadily rising, so efficiencies have to be found in other places. Those gaps hide in the data and how it’s being handled. Mismanagement, c overruns, budgeting, poor asset ROI, opaque procurement, supplies theft, and miscalculations are all areas rife with opportunity for improvements. If a business in the AEC value chain is exploiting its data thereby fully applying their data insights, it can enjoy many terrific gains. But those ignoring their data are losing out.

They are also putting themselves at serious risk. Cyber-attacks on AEC companies are rising, particularly against construction businesses operating across various sites, some of which are remote, with many devices in the field. These candy to cyber criminals. Yet some owners and managers don’t even believe they will be targeted.

Chris de Bruyn, operations director at Gabsten Technologies

However, online crime has become an illicit business that is more profitable than narcotics or weapons. Large dedicated teams plunder business accounts, and their means of attack keep evolving. Business can now be targeted through their da Ransomware is a particularly effective way to do this: just one email can result in the encryption of all the reachable company data. The cyber criminals then demand a ransom to unlock the files. Emails, customer lists, supply databases, project artefacts - all gone, bringing business to a standstill and often causing delay penalties.

It’s open season on companies that rely on data but aren’t securing that data. The same companies are also those not investigating what efficiencies their data can generate. That data is everywhere: part of desktop spreadsheets, in employe emails, on a laptop sitting in an unlocked bakkie on-site. A business that doesn’t know its data can’t explore that data to isolate opportunities for better returns and improvements. Yet, the dual challenges of security and data analytics can also support each other.

## Build a foundation with data management

By introducing a data management culture, a business can make sense of what it has and how to protect it.

Data becomes increasingly secure and useful once categorised, including sharing and coordination across different parti Every building project is a value chain of suppliers and providers - a cyberattack can target any of those. Yet, sharing the right data with partners, collaborators, clients and suppliers will achieve the best results. Knowing your data is the foundati of attaining all of the above.

You can’t secure everything, but you can ensure you’re ready for a disaster. A well-designed business continuity (BC) ar disaster recovery (DR) strategy lays the groundwork for secure and exploitable data. The plan takes shape by auditing yo data and business environments. Audit results are used to identify the types of data and components, such as device management and storage requirements. Once a BC plan is in place, and regularly tested, you are ready even if an attack happens. Extra security, analytics, and sharing services can then be added.

Times are tough for construction companies. But even as they hunker down and wait for the storm to pass, they can gain ground by analysing their data. Is it secure? Is it accessible? Is it delivering value? And, if the worst happens, can it be recovered? Answering ‘yes’ to these questions should be a priority for every AEC organisation.

## ABOUT THE AUTHOR

Chris de Bruyn, operations director at Gabsten Technologies