HOW CAN DATA CENTRE MANAGERS ENSURE CYBER-RESILIENCE?

A secure, cyber-resilient data centre is crucial to business continuity. We hear about how BaaS is becoming ever more critical, while three industry experts offer their views on how to ensure data centres are cyber-resilient.

Comport, an industry leader in business backup solutions, held a discussion about the top reasons that BaaS is critical for the security of data centres. With more sophisticated infrastructures creating more opportunities for security breaches, traditional backup may no longer be a viable solution.

"The statistics all point to outsourced backup as the solution that protects against security breaches, insufficient backup testing and a lack of staff or resources," stated Eric Young, Principal Cloud Architect of Comport. "Virtual infrastructures will only become more complex with more data to collect. The time to upgrade is now."

Some of the reasons that Comport considers BaaS critical for data centre security include:

Protecting against cybertheft: 2016 saw 4,000 unique ransomware attacks, with 15% of the SMBs experiencing an attack losing out on revenue. Digital theft is becoming more of a trend, not less. As organisations grow, they become a more tempting target for cybercriminals, companies without a BaaS solution have more to lose than they can afford.

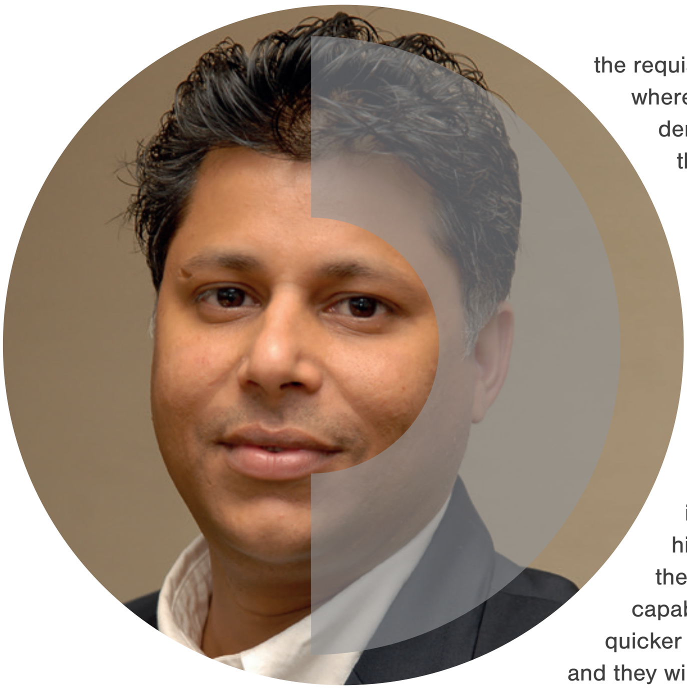
Fines for data loss: Even if a traditional backup solution is successful at recovering some of the data lost after an incident, it may not be able to mitigate fines or damaging headlines. Inadequate protection of data can cost a company millions of dollars.

Corrupted data: BaaS solutions combined with DRaaS are more effective at bringing back data in a holistic way. Information loss is the number one cost component of recovering from a cyberattack. A total of 33% of companies experience a disruption in business and 21% experience a loss of revenue.

Seamless recovery: The larger a company, the more complex a full recovery can be. Relying on a traditional backup solution gives your IT department the full responsibility for data retention and infrastructure examination.

Comport helps its customers achieve efficiencies needed to succeed in today's digital world. Customers include leading enterprises in hospitals and healthcare, financial services, manufacturing, media, retail, law firms and universities.

It has established its cloud brand, ComportSecure to help customers deal with new and emerging trends. ComportSecure specialises in solutions in cloud and managed services, advanced IT data centres, mobility security and networking.



SACHIN BHARDWAJ, EHOSTING DATAFORT, DIRECTOR

The increasing use of Big Data and the onset of the Internet of Things has only added to the intensity of the need to prioritise cybersecurity within data centres. One is also mindful of the ongoing regulations and compliance needs that have shot up. This sets the pace for a far more holistic approach to cybersecurity which comprises of a well-rounded security strategy that involves both governance and the operations angles. It includes a combination of information security, information system security as well as physical security. And the framework must be in a strong position to identify, protect, detect and respond as well as recover data.

At a time when attacks are only getting to be more sophisticated and increasing in numbers, there is evidently a gap in the requisite security professionals where supply does not match demand. It is important that data centres keep pace with the changing threat landscape and minimise the risks. Now is the time to ensure that data centres equip themselves with Artificial Intelligence (AI) and implement automation processes where the rate of identifying breaches is far higher. This will strengthen their threat detection capabilities, make them quicker to respond to threats and they will also be fortified with an analytical approach to cybersecurity. It helps in developing a far more effective, efficient and agile security posture with the added ability to forecast future threats. Service providers and end customers are investing heavily on SOC capabilities for creating an enhanced cyberdefence environment against security threats and vulnerabilities.

Visibility into the networks and the integration of advanced visual dashboards will enable clarity in what is transpiring between devices, will identify current and possible attacks as well as ensure that compliance requirements are being met. Higher network visibility will provide greater communication flow between network operations and security operations teams and will be able to proactively identify and mitigate threats. Simultaneously, workloads tend to fluctuate and organisations may not be prepared for scalability which can hinder the security environment. This calls for strong network performance monitoring tools to help reduce threats by alerting security teams of any irregular network behaviour.

While a lot is being done by data centre owners to ensure that the networks, servers and endpoint devices are secured, there is also a need to pay heed to other aspects of security that include the cooling and heating systems, power supplies and the security systems.

> Higher network visibility will provide greater communication flow between network operations and security operations teams and will be able to proactively identify and mitigate threats.