From cloud growth to a cloud mess: two out of three SMBs struggle with over-complicated IT infrastructure

As their businesses grow, companies increasingly embrace new business tools and cloud services in an attempt to make their employees' working lives more efficient and flexible, as well as reduce expenditures. According to Kaspersky Lab's latest research, nearly two thirds (63%) of companies employing up to 249 people use one or more business applications as a service. However, this trend among growing companies towards using cloud services to optimize their operations may also have negative effects, such as a loss of control over application security and valuable client data.

SMBs facilitating growth with cloud platforms

Both the smallest companies and those that are going through a rapid growth phase see cloud technologies as an opportunity to handle their business tasks in a more efficient and cost-effective way. Half (50%) of companies with up to 49 staff members (VSBs) and 40% of companies with 50–249 staff members (SMBs), have employees who regularly work outside of the office and need access to data and applications via the cloud. And, as companies become larger, they experience a growing need for cloud services: 73% of SMBs and 56% of VSBs use at least one cloud service. Among the most popular SaaS tools are email, document storage and collaboration services, finance and accounting.

IT, cybersecurity and a lack of control

However, an active use of clouds has a flipside to it as well: IT infrastructures in organizations are increasingly consolidating more services and applications, but at times they fall short of providing the required levels of control and visibility. As a consequence, 66% of companies having 1–249 staff members experience difficulties around managing these heterogeneous IT infrastructures.

This growing complexity requires SMBs to take a new approach to infrastructure management. The problem, however, is that in-house IT specialists do not always have sufficient expertise to meet this challenge. Moreover, 14% of companies with 50–249 employees trust IT security management to staff members who are absolutely not IT specialists. This can result in the emergence of real risks to the companies' cybersecurity that they may not always be able or have time to assess, as they focus most of their attention on developing their businesses.

Who is responsible for data protection in the applications consumed as-a-service?

Even in the context of information security functions proving to be secondary to business growth, SMB companies are still conscious of how important it is for them to ensure the security of their client's valuable data. For both VSBs and SMBs, data security is the number one challenge that they have to deal with. However, in 49% of VSBs and 64% of SMBs, valuable client data is stored on staff members' mobile devices. Leaking this data has the potential to result in serious damage to the reputation of the company, as well as financial losses resulting from litigations. While Enterprise-level companies normally have reserve resources with which to weather out such difficulties, smaller organizations may face dramatic consequences, such as serious disruptions in operations or even

lost business.

Although small companies are conscious of the problem, they do not have a clear understanding of who bears the responsibility for these assets, since they are being processed in cloud services. Companies with up to 49 staff members show an especially disturbing attitude to this problem. For example, nearly two thirds (64%) of VSB respondents are convinced that the provider is responsible for the security of document exchange applications, while 56% of SMB respondents share this opinion.

“To enjoy the advantages of cloud computing regardless of the growth stage they are in, businesses need to effectively manage an array of cloud platforms and services. Fundamental to this is being able to clearly recognize who is responsible for cybersecurity in IT infrastructures that are continuing to increase in complexity. Whether it is managed by internal staff or trusted adviser, cybersecurity cannot be overlooked”, says Maxim Frolov, Vice President of Global Sales at Kaspersky Lab. “All businesses should therefore establish a dedicated role within which the security of cloud platforms, sensitive data and business processes are kept under control”.

To maintain cybersecurity at each stage of business growth, Kaspersky Lab offers a portfolio of solutions that have been specifically developed for organizations of any size – from small startups to actively growing and more mature companies. In accordance with the growing trend of using clouds, in Kaspersky Lab portfolio, there are security solutions that can be deployed and managed from the cloud, as well as special products to protect cloud applications.

For more details on the challenges facing small and medium sized businesses as they grow and embrace cloud technologies, please read our latest report.