Brought to you by: CIO FROM IDG

CAN YOU HANDLE GROWING CYBERTHREATS?

KNOWING WHEN TO TURN TO EXPERTS TO KEEP YOU SAFE

Security is paramount in every organization. But should it still be managed within the enterprise?

No longer a "check box" consideration, cybersecurity is a business enabler encompassing critical applications, data, and reputation. Increasingly, enterprises must ask themselves whether they can afford to shoulder this responsibility alone.

Outsourcing noncore functions and business processes is nothing new, but IT security has often been considered too sensitive to entrust to outsiders. Today, though, the complexity of quickly evolving IT architectures is too much for many organizations to continue to handle internally. Meanwhile, specialized managed security services providers (MSSPs) have the resources and the ability to maintain intense focus on protecting their clients' business-critical data.

The need to secure data across a multi-cloud environment is a strong justification for turning to a managed cloud provider. The ability to aggregate infrastructure, expertise, and scale around a rapidly changing architecture is often beyond the capabilities of many enterprises.

Heightened focus on risk

As *CIO* observes, "Many small and midsize companies are gravitating toward an outsourced model for security and day-to-day operations, given the increasing number of data breaches and the heightened focus on risk." According to that article, a recent survey of 287 U.S.-based IT and business professionals reveals that 40% of respondents are turning to MSSPs.

In a recent Q&A with *Network World*, Rackspace CEO Taylor Rhodes says the company's fastest growing businesses are in managing third-party public clouds and cybersecurity. There's a key difference to an enterprise handling security by itself, in isolation, and a service provider that can see a broader picture.

"We get to aggregate a lot of knowledge and expertise and visibility across thousands of customers, and build the combination software/hardware and services around cybersecurity at scale, so that our customers don't have to invest in all of that capability for themselves," says Rhodes.

TO DIY OR NOT TO DIY, THAT IS THE QUESTION

Many organizations are invested in a do-it-yourself (DIY) approach to security. Like other aspects of IT, though, this approach should be continually reevaluated considering growing threats and changing realities.

Ask yourself if your organization is well positioned to deal with the following:

- Increased compliance and audit demands
- Lack of trained security professionals in the market
- Rapid growth and lack of integration in security tools
- Increased adoption of multi-cloud environments
- Declining overall IT budgets

WRAPPING IN SECURITY

Utilizing a cloud-based provider that can offer security services as part of a comprehensive portfolio brings additional benefits. "We're able to match the workload with the best infrastructure solution, and then wrap that in value-added services like managed security and deliver that as a fully managed service with SLAs that are clearly articulated and industry-leading," says Rhodes.

Still, as the CIO article points out, 60% of those surveyed have not turned to MSSPs, at least not yet. That's not surprising, given how long it took for many enterprises to warm up to cloud providers for key IT functions. But enterprises have increasingly moved to cloud as they shed infrastructure costs that are not central to their business focus.

Ask yourself if you want security to be your business focus, or if you'd be better off turning to specialists who do indeed make it their business.