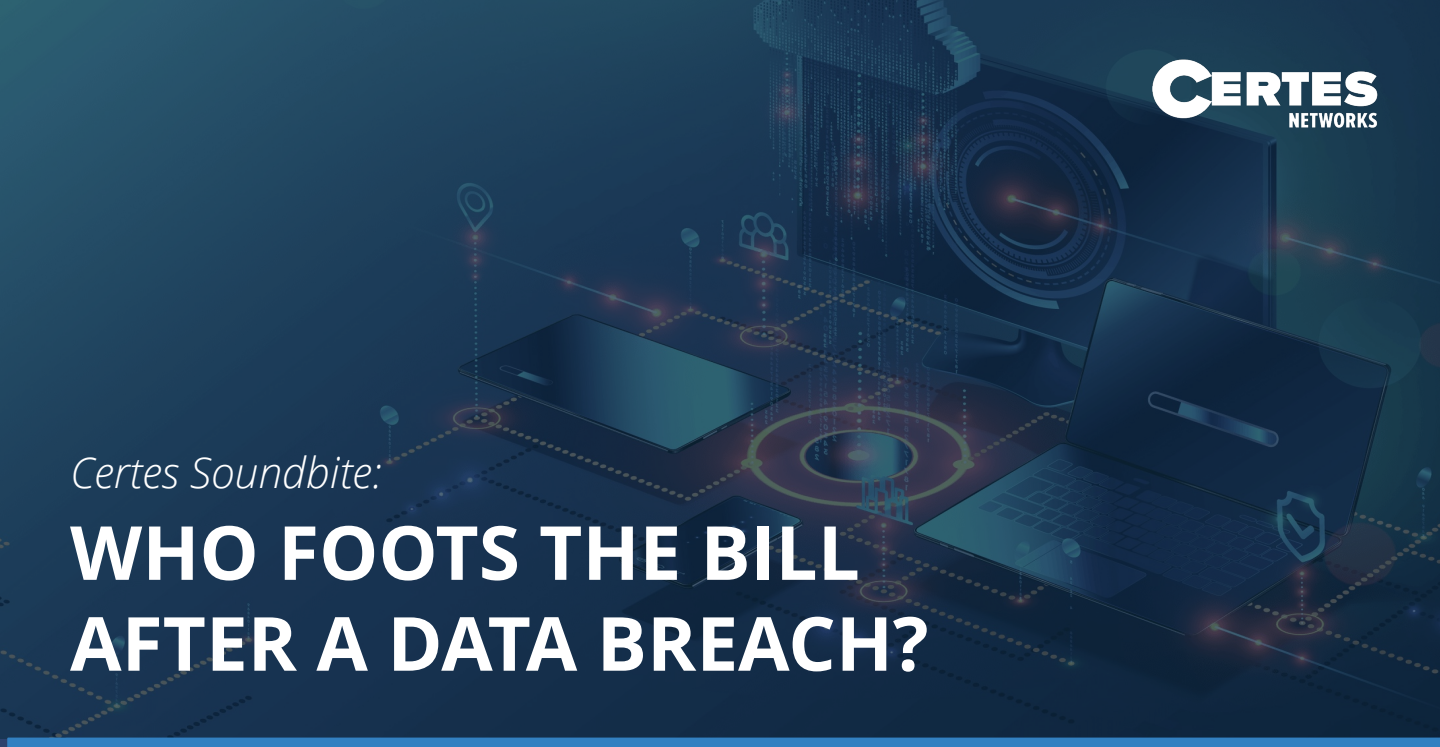

Certes Soundbite:

WHO FOOTS THE BILL AFTER A DATA BREACH?

Data breach is almost inevitable – which means it is vital that companies and their Managed Services Providers (MSPs) understand exactly who is responsible and who bears the financial brunt. But recent research reveals that both companies and MSPs are disturbingly unclear about their legal and financial obligations. Contracts are ambiguous and the risks of legal wrangling severe. The truth is that when a breach occurs and data is exposed, neither party wins. As Simon Pamplin, CTO, Certes Networks, insists, rather than playing the blame game, the priority must be to protect the data to ensure that even when an attacker breaks through, there is nothing to see and nothing to gain.

Financial Burden

Cyber security has become a board level issue in recent years – not least since the introduction of ever more punitive fines and personal responsibility for the protection of sensitive data. Yet recent research undertaken by Sapio Research on behalf of Certes Networks confirms that far too many businesses are simply handing over responsibility to an IT Service Provider (ITSP) or Managed Services Provider (MSP) – and expecting the provider to pick up the financial cost should a data breach occur.

Companies employing third party organisations to deliver security policies expect ITSPs to cover 48% of the costs in the event of a data breach. Astonishingly, 73% of ITSPs also consider themselves responsible for paying fines and damages and believe they should pay 51% of the costs.

Whether these expectations can be met as and when a breach occurs remains a legal minefield. More critically, for senior managers personally liable for security and information protection compliance, does this abdication of responsibility to a third party stand up to regulatory scrutiny?

> *It is naïve to expect a network security infrastructure expert to understand the full implication of financial and reputation loss associated with a data breach. It is not in their remit. They are responsible for the performance of the infrastructure – not the value or assurance of corporate data.*
>
> **Simon Pamplin, CTO, Certes Networks**

Endemic Misperception

How does a reliance on an MSP or ITSP support the zero-trust approach to separating policy responsibility from system administration? Any security posture needs to be defined from a business standpoint to reflect the sensitivity of specific data sets. But if the onus is placed on the MSP, the entire security posture is both defined and delivered by a network security team. Contractual agreements will be meaningless if a regulator comes down hard on this clear lack of Separation of Duties.

Furthermore, the legal standpoint is that the data owner is responsible and liable for any data breach – so any company with the misperception that the MSP or ITSP will foot the bill is likely to be in for a very nasty surprise. This perception indicates that far too many companies are not considering the true implications of data security at the right level.

Are the data protection and compliance officers, as well as senior managers, now personally liable for protecting sensitive company, customer and partner data involved in these decisions? If so, do they really believe that asking the network security team to appoint an MSP to provide an SD WAN is really an adequate approach to data protection and compliance?

Demanding Safeguards

It is naïve to expect a network security infrastructure expert to understand the full implication of financial and reputation loss associated with a data breach. It is not in their remit. They are responsible for the performance of the infrastructure – not the value or assurance of corporate data.

Companies need to take ownership of their data – and that means demanding the MSP or ITSP provides another level of data protection. An MSP that wraps security around the data, rather than relying on the network infrastructure, can provide business leaders with the essential assurance that data is protected and compliant.

Rather than playing the blame game, the priority must be to protect the data to ensure that even when an attacker breaks through, there is nothing to see and nothing to gain.

Simon Pamplin, CTO, Certes Networks

Adopting Layer 4, policy-based encryption ensures the data payload is protected for its entire journey - and because only the payload data is encrypted while header data remains in the clear, means minimal disruption to network services or applications. With encryption policies based on the sensitivity of corporate data, the business can achieve a clear separation between policy setting and systems management. A win for both data officers and network security teams.

Conclusion

This research raises a very concerning issue for both companies and ITSPs/ MSPs. Whoever ends up footing the bill – and the chances are that a lengthy court case could ensue – no one wins. Any data breach will incur not only immediate financial costs but long-term business consequences that could be devastating for both parties.

So why risk it? If a company takes a different approach and demands that additional data protection layer, there is no longer any issue of blame or cost. The company is no longer relying on a third party to safeguard its data, but instead taking ownership itself. By encrypting data, in a way that doesn't affect business operations, it is safeguarded across whatever infrastructure the MSP or ITSP is providing.

Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

CERTES NETWORKS

Tel: 1 (888) 833-1142
sales@certesnetworks.com
www.certesnetworks.com