3 steps to ransomware risk mitigation

By Kate Mollett

3 Nov 2021

Ransomware is currently a hot topic, and has become an everyday threat that affects the lives of everyone, not just corporations. Case in point is the recent attack on the Department of Justice, which has been an ongoing challenge that has affected aspects such as maintenance payments, bail services and even letters of authority required for funerals and estates. The prevalence of ransomware is increasing exponentially, and it has become critical for organisations to plan for 'when' it happens, and not 'if'. In a world where we are more interconnected and reliant on technology than ever before, we are also more vulnerable, so a multi-tiered approach to cybersecurity is essential.

Kate Mollett

The current challenge

The cyberthreat landscape is something of a perfect storm at present. With the pandemic, the number of places data resides has increased, along with the number of employees working on edge devices, and the growing prevalence of the cloud. This has vastly increased the attack surface, making targets easy to hit and highly lucrative for cybercriminals.

There is also the challenge of different environments, from legacy databases to cloud platforms, all of which have different requirements but must be considered as part of a holistic cybersecurity approach. The IT landscape is constantly evolving, and the threat landscape is evolving in tandem to the point where ransomware is no longer only a threat for high-profile organisations. Ultimately, businesses need to ensure that they are able to recover from an attack, which requires a three-step approach of protection, recovery and reform.

Protect

Data protection is the foundation of cybersecurity, but this is not just about having a backup in place. Data management is critical, because unless organisations know where their data is, what the data is, and what level of importance it carries for the business, it cannot be effectively protected.

When it comes to data management, many enterprises employ multiple disparate technologies. The challenge here is that this inevitably creates a fragmented view of data, which makes recovery from an attack more difficult. Integrating data is critical, and this requires a single pane of glass data management platform to help businesses identify, categorise and then protect data in the most efficient way possible.

The key to effective recovery is effective protection from a single integrated solution that ensures that data is secure, clean and air-gapped, to provide a level of assurance that if and when it is needed for recovery, it will not infect or reinfect the network. However, protecting data is not sufficient in isolation. Constant monitoring and analysis of data has become equally crucial, using artificial intelligence and machine learning algorithms to deliver better control and visibility, and a holistic view of data.

The aim of data protection is to mitigate the need to recover. To deliver a level of confidence in the solution, preparation is the key and regular testing is vital. The IT environment is constantly evolving, which means that any disaster recovery plan must be regularly assessed to ensure it continues to work in this changing environment.

Recover

Inevitably, an incident will occur, whether this is a ransomware attack, a data leak, a natural disaster or any other incident. The way organisations respond will determine their recovery time. Not only is it essential to have the right backups in place, it is also vital to have an incident response plan in place, with procedures that have been practised and that scale depending on the nature and severity of the incident.

Working with vendors and partners becomes necessary to analyse the extent of the vulnerability and to verify the integrity of the backup before it is restored. This is an important step in ensuring the backup of the right data is reliable and that the data itself is clean. This aspect should never become a tick-box exercise; it needs to involve the entire business, as well as vendors and partners, to develop a complete business continuity approach, including a communications plan on how to manage an incident. The key is to be prepared and to plan for the worst.

Reform

Finally, we need to remember that data protection is not only about preventing ransomware. There is still the element of legislation that needs to be taken into account, which should be top of mind with the Protection of Personal Information Act (PoPIA) becoming enforceable. Legislative compliance and ransomware protection both benefit from a multi-layered approach to data management and data protection, and one that emphasises that organisations are ultimately responsible for their own data assets.

Falling back on cyber-insurance policies or budgeting for the payment of ransoms will not solve the problem and will likely only encourage cybercriminals further. The reality is that the threat is not going away, and it has become essential to have the right underlying systems and processes in place to mitigate risk as much as possible. This means working with technology partners to stay ahead of the game and keep data management top of mind.

ABOUT THE AUTHOR

Kate Mollett is the Regional Director at Commvault Africa