Ransomware Backup & Resiliency Assessment

FENIX24®

Assessments are a useful tool for Incident Response preparation, but often they do not provide realistic preparation for an actual ransomware event because they are based on assumptions about data survivability, immutability, and MTTR (Mean Time To Recover) and not on a realistic assessment of how a company's infrastructure and backups will survive todays' modern threat actor attack. But we know from experience that these assumptions are usually wrong.

Fenix24 has developed a fundamentally different assessment. Based on our real-world experience as the worlds' leading ransomware recovery experts, we analyze your backup configurations and resiliency through "shoulder-surfing" so we can tell you how your company's backups and infrastructure will actually perform in the face of a modern threat actor.

What will survive? What won't? How long will recovery take and what are likely to be the key bottlenecks? The assessment concludes with an interactive executive experience and presentation of findings. Companies will be better prepared for the reality of a ransomware attack, and empowered to know what you can change before the attack to reduce the destruction and business interruption that results from modern day ransomware.

The Focus: Your Survivability and Recoverability

Ultimately the key to organizational resiliency is understanding both **what** will survive and attack and **how long** it will take for you to recover. In order to understand these, we will assess:

How much of your data will survive? *Rarely is it 100% even if ransom is paid*

Will your backups survive/be usable? *80% of backup presumed immutable do not survive*

Will your infrastructure including AD survive? *In order to rehydrate recovered data and validate identity*

Do you have sufficient storage, bandwidth and connectivity? *Necessary in order to restore quickly*

Our approach digs deep into each of these questions in order to provide you with a realistic assessment of exactly what of your data and which applications will survive and be usable, as well as a multi-step timeline for your recovery.

"**Cyber resiliency** is now a requirement of both Board Members and Corporate Officers under Delaware Law, and the **key to resilience is recovery**. This is the only Tabletop I've seen focused on recovery, and it's offered by the leading ransomware experts in the world."

—ANDY SERWIN, DLA PIPER, US CHAIR DATA PROTECTION

1.855.FENIX24 | www.fenix24.com | rapidresponse@fenix24.com