by Paul Balkwell, Vice President of International Sales, Continuum

Global ransomware damage costs are skyrocketing, reported to exceed £10 billion by 2019. But, it may surprise organisations to learn that ransom payouts could be the least of all damage cost contributors. The real financial injury is in the post-attack disruption to a business’ operations and productivity.

With a comprehensive business continuity plan in place, an organisation has a better chance of significantly reducing downtime from a ransomware attack. Unfortunately, while organisations may think they have a proper plan in place for when disaster strikes and data needs to be recovered, many actually have gaping holes in their BDR and security strategies that they don’t even know exist. This is especially true in the SMB sector, as key decision makers are typically focused on core business issues such as serving clients and optimising growth, and don’t consider backups a top priority.

In the face of increasingly devastating cyberattacks and other types of file loss, managed service providers (MSPs) have the opportunity to position themselves as a trusted partner for SMBs and optimise their own business growth by offering robust business continuity services. However, many MSPs jeopardise their long-term profitability and gamble with the safety of their clients' data because they fail to avoid these common BDR pitfalls:

#1 – Assuming Your Clients Appreciate the Critical Business Cost of Data Loss

Despite increased coverage in mainstream media of devastating breaches and data loss incidents, there are still many organisations, particularly in the SMB market, that believe data loss doesn't pose a serious risk to their business. This is concerning as hackers often see small and medium sized businesses as an easy target. The reason being, they lack the funds to secure sufficient IT protection and often have no choice but to pay to get their data back. With the majority of businesses closing their doors within a year of a data loss incident, for any business, let alone an SMB, the damage done by one data breach could be insurmountable.

What your clients don't know could destroy their business. It's the MSP's duty to properly educate their clients on the magnitude of the financial risks associated with cyber-attacks. MSPs must ensure that their clients fully comprehend the critical impact these events can have on a businesses' reputation, customer base and even employees (depending on the organisation's ability to recover and restore systems).

#2 – Not Integrating BDR With Your Client's Security Strategy

As cybersecurity and vulnerability management become critical functions in both the enterprise and the SMB, it's important for MSPs to understand the role of an effective business continuity strategy in a larger security ecosystem.

MSPs must acknowledge that preventative measures could fail and that BDR is the ultimate cyber-attack failsafe. From a security perspective, a BDR strategy must be in place prior to an attack in order to minimize downtime and the loss of recent work. MSPs should bundle or promote BDR offerings alongside security solutions to provide true end-to-end data protection services to customers.

#3 – Thinking Regular Backup Testing and Verification Isn't Essential

If MSPs don't conduct frequent backup testing and verification, they won't be able to ensure that their clients' backups are configured properly. As a consequence, they only find out that the

backups don't work when their client encounters a real data breach or extended outage—and by then it’s too late.

Additionally, MSPs who incorporate simulated disaster recovery into their managed services agreements will successfully differentiate themselves from other MSPs and avoid fire drills with their customer. MSPs should ask prospects if their current IT service provider offers tests to verify that the restoration process works. If not, this could become your unique selling proposition.

Backup verification is usually a software-driven exercise, relying on both technology and human resources to confirm that the tech and systems powering a backup and disaster recovery strategy will function properly when needed. This includes verification of the actual boot or startup process for any virtual machines or recovered data, as well as confirmation that any redundant or failover systems will activate properly when needed.

#4 – Failing to Separate Backups from Your Clients’ Main Infrastructure

When building a business continuity strategy, it’s critical that backups are isolated from a clients’ primary infrastructure and power supply. This is particularly true in the SMB market, where there is often only one office or location where all business is conducted.

If a backup appliance is on site, for instance, it’s wise to maintain additional redundancy in a cloud environment to ensure data can be accessed in the event of a significant power failure or disaster that takes an entire business offline.

#5 – Relying on File-Based Solutions to Save You in a Disaster Recovery Scenario

File-based sync and share systems such as Dropbox and Google Drive should not be mistaken as full-fledged business continuity technologies, as they offer very basic and rudimentary backup capabilities and aren’t well-suited for entire system restores or virtual machine creation in the way that modern BDR platforms are.

These services can act as a suitable band-aid for an individual user whose computer suddenly stops working one day. However, MSPs should be prepared to properly explain when pitching to potential customers that these services should not be relied on as a means of maintaining complete business continuity in the event of a disaster.

#6 – Failing to Have a Recovery Plan in Place When Disaster Strikes

Complete disaster recovery simulation takes the concept of backup verification a step further, and requires a careful examination of any internal processes, procedures and instructions that should be followed in a data loss scenario. Only when a response policy is put to the test can an MSP adequately assess the effectiveness of their clients’ disaster recovery plan.

Technology alone won't save a client paralysed by an IT emergency. MSPs should advise their clients to consider continuity of operations and business processes in addition to data restoration. Being properly prepared can be as simple as knowing who to call and having an up-to-date contact list. MSP’s should also advise that disaster recovery plans avoid ambiguity and expectations should be set when it comes to designating team and individual roles and responsibilities.

#7 – Taking a One-Size-Fits-All Approach To Clients’ BDR Needs

When delivering business continuity services, no two customers are likely to have the same backup requirements—and trying to deliver the same exact offering to everyone can present a series of challenges.

To avoid these headaches, MSPs should look to leverage a platform that’s capable of meeting a diverse range of customer needs. Many organisations have specific compliance and regulatory statutes that they're required to adhere to. No two clients are alike and BDR processes and procedures should be optimised for each individual client’s objectives. Providers should also consider offering a few different packages or service options to attract a wider audience.

Building a Successful Business Continuity Strategy

The risks and damages associated with a data loss incident are too severe to be ignored and an aggressive cybersecurity landscape has heightened the need for effective business continuity planning as a last line of defense.

By avoiding these common BDR pitfalls, MSPs have the opportunity to alleviate SMBs’ fears of data loss and downtime. Smart MSPs can set themselves apart from the competition by acting as an extension of their clients’ business and providing higher level data management, protection and business continuity expertise.