rhipe

# The MSP guide to shifting perceptions of Business Continuity

# The MSP guide to shifting perceptions of Business Continuity

Almost everyone who works in the technology industry understands the concept of business continuity, its components, and why it's so important. It's something we've been aware of and educated about for a long time. It's our job to know.

Your customers, not so much - especially small and medium businesses (SMBs). It's not their job to know (or not their day job). Their job is to make sales, satisfy customers, build new products and services, manage finances and lead teams. Leaving not a lot of head-space for Business Continuity (BC). Therefore, it falls to you to help educate your customers about why Business Continuity is just as essential to their business survival as satisfying their customers and other stakeholders.

## The current SMB perception.

Unfortunately, Business Continuity can seem an uninspiring, unexciting term. The Collins Dictionary defines continuity as: "the fact that something continues to happen or exist, with no great changes or interruptions". It is hard to blame your customers if that doesn't exactly quicken their pulses.

You need to rebrand BC as being about the two most important and connected goals of any SMB: business survival and business growth. SMB owners want to grow, but without the certainty of survival there can be no growth. When you educate your customers that business survival and business growth depend on business continuity, you can create a sense of urgency, and a desire to invest.

Your challenge now is to redefine BC as a business priority. You must explain the threats that make BC essential; break down its key components, and offer simple, cost-effective strategies and solutions.

Business Continuity solutions are crucial in every MSP's modern cyber-resilience strategy and technology stack as they represent a growth market. Without them, you are vulnerable to losing business to competitors who have such offerings. And your customers are at risk of losing important data, suffering costly downtime, and potentially leaving you liable.

# The SMB risk: Money talks, when data walks

Two well-documented megatrends have led to the critical importance of Business Continuity: firstly, our almost total dependence on technology in business and government, and second, the addition of cybercrime to traditional disruptors of technology services such as equipment malfunction and human error.

## More places, more problems. Protecting your customers data.

Our economy's almost total dependence on "always on" technology has elevated the risk of technology disruption. Consulting giant Accenture says almost 100% of companies rely on the internet for business today, while 10 years ago it was just 25%.

Previously a tech outage may only have affected back-office apps like accounting, now it can bring down the parts of the business customers rely on: web-based sales, support and services. Every minute or hour lost means customers potentially going to competitors. Days or weeks lost may mean the business fails.

Following the COVID-induced move to Working from Home, most businesses are dependent on remote employees – if they are denied access to networks and apps they can't work effectively and can't service the business's customers. It's crystal clear that no business continuity plan can quickly lead to no business remaining.

**In Australia, a cybercrime is reported every**

**10 Minutes**

THE SMB RISK: MONEY TALKS, WHEN DATA WALKS

## Disruption, Disaster and Data Loss comes in many forms.

Businesses were at risk from technology disruption long before the term "hacking" entered the dictionary, and that continues today. These threats include employee errors such as deleting files and folders and downloading non-approved virus-ridden apps. Employees with malign intent can steal money or destroy critical information from inside.

Data loss can be caused by many different factors, and each poses a unique problem for data recovery. Over two-thirds (67%) of data loss is caused by hard drive crashes or system failure, 14% is caused by human error and 10% is a result of software failure.

These risks have always been with us, and prudent businesses have always taken precautions with Disaster Recovery (DR) plans including mock disaster simulations where recovery plans are enacted, tested, reviewed and updated. Such rehearsals are an important tool for ensuring BC plans are real.

The recent emergence of industrial-level cybercrime, with sophisticated criminal gangs using technologies like Artificial Intelligence (AI) to maximise their potential for success, has ramped up the risk to businesses large and small.

THE SMB RISK: MONEY TALKS, WHEN DATA WALKS

## Internet-connected devices can be attacked thousands of times a day.

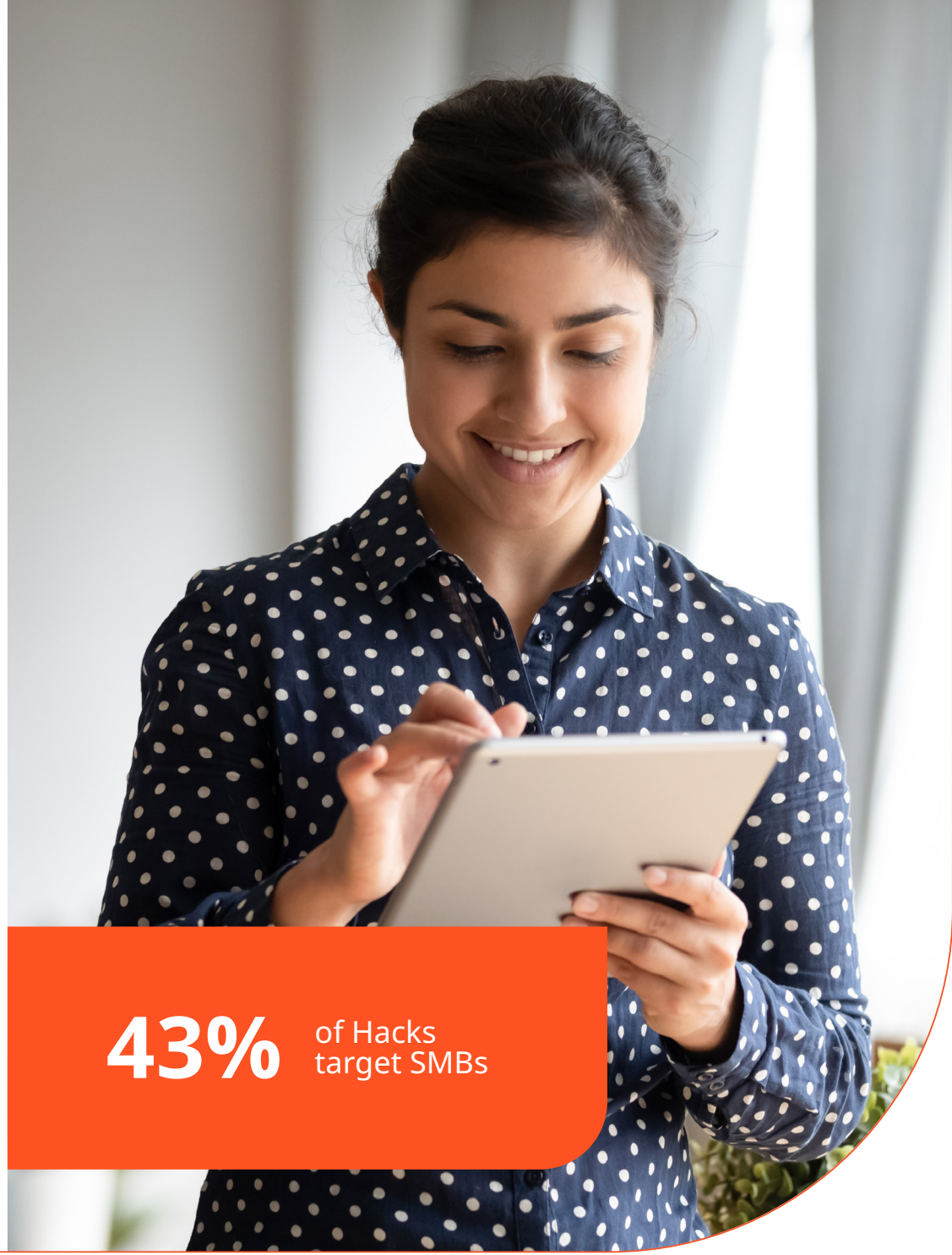
As far back as 2017, Security Magazine reported that:

"a study at the University of Maryland was one of the first to quantify the near-constant rate of hacker attacks of computers with Internet access—every 39 seconds on average—and the non-secure usernames and passwords we use that give attackers more chance of success."

The Maryland study reported hackers used automated hacking techniques to enable the mass hackings and revealed how often devices' defences are tested: "The computers in our study were attacked, on average, 2,244 times a day." Four years later such attacks have grown.

The sheer scale of these attacks is similar elsewhere and is a global threat to SMBs. Insurance business Hiscox reports around 65,000 attempts to hack SMBs in the UK every day, with around 4,500 being successful. That equates to one SMB in the UK being successfully hacked every 19 seconds.

This data should cause every SMB leader to sit up and take action – if your customers don't have a robust BC plan in place they have a high chance of being breached. As a technology professional, knowing the risks you almost have an obligation to make sure they also fully understand the risks.



# The road to recovery can be costly

Comparatively the cost of recovery can cost tens of thousands, hours of work and potential risk of customers.

## Businesses suffer because they don't understand the risks or ignored it completely.

The damage ranges from fatal (Inc.com reported in 2018 that 60% of hacked businesses go belly-up within 6 months) to severe, such as an average of 16.2 days downtime to recover data and restore networks following ransomware attacks. Indeed, 16.2 days downtime would be fatal for many businesses.

Attacks on SMBs make up a high proportion of total hacks, between 40% to 70% depending on how it's measured. This is partly due to inadequate precautions by SMBs (62% don't have up-to-date BC strategies), and partly because larger corporations, spurred by regulatory guidelines and specialist in-house IT security professionals, have implemented tighter BC defences thus encouraging hackers to turn their attentions to less defended SMBs.

**Only 14%** of SMBs have adequate cyber security defence

**60%** of SMBs that get hacked go under within 6 months

**More than 60%** of hacked businesses are hacked again within 12 months

# Wishful thinking isn't an effective data protection strategy

Threats and related impacts confront enterprises, government organisations and SMBs, but with different levels of intensity and priority.

## Ignorance of risk is the real risk.

Typically, enterprises and government organisations have legal and compliance drivers that force them to deploy BC measures. Most SMBs other than listed businesses, do not.

Despite the proven pain and costs of data loss – from whatever incident - many SMBs don't think they are at risk. The Cyber Security and Australian Small Businesses study from June 2020 by The Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC) surveyed 1763 SMBs and told a tale of two tribes:

- Of the SMBs who'd never previously experienced a cyber incident, only 9% believed they were "almost certain" to experience an incident in future
- However, fully 48% of respondents who'd previously experienced a cyber incident believed they were almost certain to experience another in future.

62% admitted they had previously experienced an incident. This is strong evidence that the BC market will grow quickly because SMBs that have previously suffered an incident at least believe security is a threat, and as that proportion of SMBs grows – as it will – there will be more awareness and propensity to buy.

Some SMBs can accept they're at risk but don't want to address the elephant in the room, or just think it's in the too-hard basket.

**A ransomware attack causes an average of**

**16.2 days** of downtime due to recovery of data and restoring networks

# Overcoming the Business Continuity Barriers

MSPs must first understand the types of barriers that SMBs face before offering strategies for Business Continuity.

## Unpacking the too-hard basket.

The ACSC study revealed some key barriers to implementing good cyber security practices. These barriers presented provide strong arguments for MSPs to use when engaging SMBs on BC.

### Lack of dedicated staff

Cyber security has to compete for time and other resources with multiple demands.

### Planning & responding

Businesses need to better plan to respond to cyber incidents and data loss.

### Complexity & self-efficiency

Business owners fail to identify weaknesses in security practices and know they are struggling but don't know where to begin.

### Underestimate risk

Businesses need to better understand the risk and impact of cyber incidents and data loss and stop underestimating their recovery time after the incident.

OVERCOMING THE BUSINESS CONTINUITY BARRIERS

## The same survey also provides some compelling insights into why SMBs are at risk:

- Almost half of SMBs rated their cyber security understanding as 'average' or 'below average' and had poor cyber security practices
- Almost half reported they spent less than $500 on cyber security per year
- 62% of respondents admitted experiencing a cyber security incident.

## MSPs can engage SMBs by:

- Explaining the size of the risks
- Helping SMBs navigate the complexity of today's technology
- Assist in creating BC plans
- Where appropriate, provide expert staff to overcome dedicated IT staff shortages in SMBs.

All these initiatives provide opportunity for new solution sales and services revenues.

# The journey starts with three easy steps!

Given the many barriers to SMBs addressing BC, an optimum strategy for a first engagement is simply to start with initial clear needs and go for some quick wins.

## Start with cloud backup.

Each SMB will be different but there are common themes, and everyone needs reliable off-site backup. This gives the client certainty they at least have the business's key data secured. It also gets the customer thinking with a business continuity mindset and should open them up to a more strategic approach. Backup is the crucial foundation for a layered, cyber-resilience strategy in an increasingly threat-heavy IT landscape.

## Next do a BC audit.

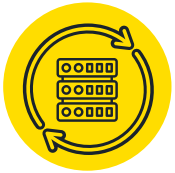
Where possible use a checklist (see below) to identify the customer's starting position and priorities. This serves as the basis for a BC plan where you can help the client identify strengths and weaknesses in their current BC position and focus on fixing the highest priority areas. This isn't a lengthy exercise, it's just a one or two-day consulting session with the leadership team, and a short document that defines current BC readiness.

- **Who is responsible for Business Continuity in your SMB?**
- **What does your Business Continuity and disaster recovery plan look like today?**
- **How often is it reviewed and updated?**
- **How long can your business afford to be down?**
- **Does your business know where all your critical data resides (on-premises, across various Cloud and SaaS providers etc.)?**
- **How much data can your business afford to lose?**
- **Have you or anyone you know experienced a ransomware attack or downtime due to hardware failure?**
- **Are you currently backing up email and cloud applications?**

THE JOURNEY STARTS WITH A SIMPLE STEP

## Establish Business Continuity Tools.

Answers to these questions will help establish which Business Continuity tools (see rhipe Solutions on page 13) are required to meet the specific requirements. Choosing the perfect solution isn't always easy, there's a lot to consider and many features to compare. Find the right blend to meet the unique customer needs. Consider the different elements of Business Continuity when designing the solution.



**Backup**

**SaaS Backup**

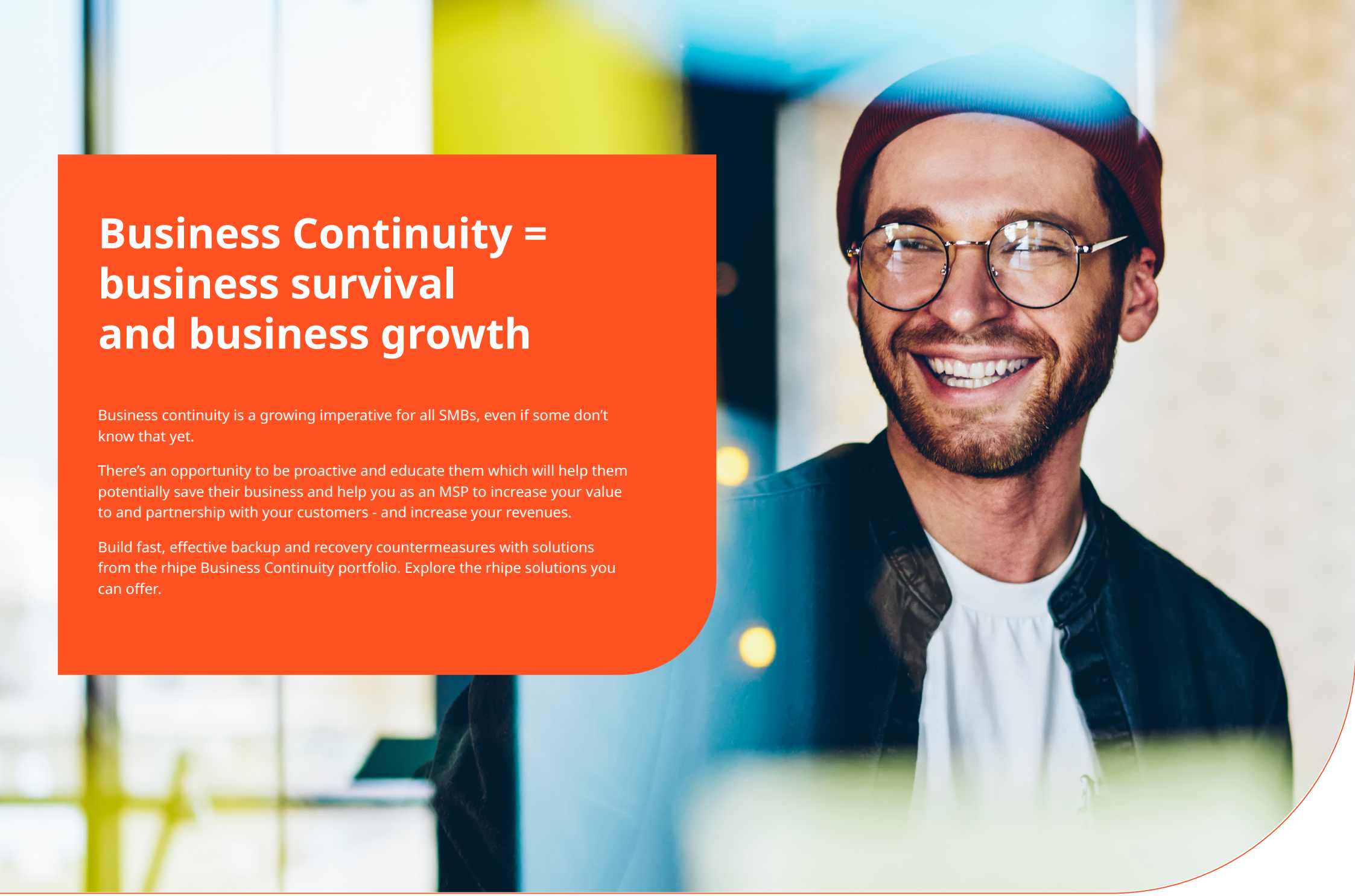
**Storage**

**Email Archiving**

**File Sharing**

**Disaster Recovery**

**Automation & Remote Management Tools for MSPs**



# Business Continuity = business survival and business growth

Business continuity is a growing imperative for all SMBs, even if some don't know that yet.

There's an opportunity to be proactive and educate them which will help them potentially save their business and help you as an MSP to increase your value to and partnership with your customers - and increase your revenues.

Build fast, effective backup and recovery countermeasures with solutions from the rhipe Business Continuity portfolio. Explore the rhipe solutions you can offer.

# rhipe Solutions you can offer

**Explore rhipe's Business Continuity solutions and find the right fit for your tech stack.**

| | | |
|---|---|---|
| **Migration** | Do more than just the standard lift and shift and add value by sanitizing your clients data and structures during migration. Saving you resources, time and money and improve security and long-term management of your clients data. | skykick, AvePoint |
| **Microsoft 365 & Office 365** | Microsoft 365 has a few short-term recoverability options like the Recycle Bin and soft deletion, but it doesn't include long-term recoverability options! | skykick, AvePoint, Acronis, VEEAM, BACKUP365 |
| **Microsoft Dynamics 365** | Dynamics 365 backups up once a day on a fixed schedule but can only restore at the instance and sandbox instance levels. It's important to explore Backup solutions that can provide flexible and in depth data retention and restoration. | AvePoint |
| **Azure** | While Microsoft assumes responsibility for the infrastructure, their Shared Responsibility Model makes it clear that it is still your data and you retain the responsibility to secure and protect it. | Acronis, VEEAM |
| **VMware** | For VMware backup, there are different levels of VMware that can be protected — ultimately based upon what your needs are to meet your recovery objectives. | Acronis, VEEAM |
| **Google Backup** | Google's cloud provides server redundancy and short-term recovery via a Trash bin, but actual retention options to protect your information are limited. Google encourages you to protect data via a backup partner to secure user data for long term protection. | AvePoint, Acronis |
| **Security & Compliance** | There is no gold-standard for vendor best practices. Each technology and product you use has its own best practices. Security audits are becoming more frequent, and the cost of noncompliance is increasingly more expensive. | AvePoint, Acronis, Runecast |


rhipe
Expertise that Empowers
rhipe.com