# How to choose backup for SMBs

ebook

www.technologydecisions.com.au

technology Decisions
IT leadership & innovation
www.technologydecisions.com.au

WESTWICK-FARROW MEDIA

Here's a basic business rule that almost everyone learns the hard way: backups matter. After spending most of the last two decades working in enterprise IT, there have only been two occasions when anyone has cared about backup. Once was when a disk failure and someone's inattention to an alert in a backup log meant that the CEO lost his entire calendar and the other was when the HR manager in another business lost the CEO's salary information.

Today's computing environment is complex. Data is kept locally on servers, on computers, tablets and in the cloud. And, to paraphrase Spiderman, with great flexibility comes great complexity.

That complexity means that the way we back up our distributed and virtualised environments has to change from the way we did it just a few years ago. While the same rules of testing backups and storing them off-site, away from our core systems, are still important, we need to ensure that our tools protect our precious data and applications.

After all, if your business lost critical data could it keep operating? Or are those sorts of systems problems something that could only happen to someone else?

Anthony Caruana,
Editor – *Technology Decisions*

# Contents

# Backup for SMBs

*Anthony Caruana*

What would happen to your business if you lost access to critical customer data like orders and invoices? What about that important proposal you've been working on for the last three days? Or, worst of all, there's a fire and all your computers are destroyed? How long could your business survive in such a situation?

For many businesses, these are hard questions that are rarely asked. And given the increasing complexity of our technology footprint, the answer might not be easily discerned.

According to John Reeman from Symantec, "Businesses need to be serious about their disaster recovery planning. Most businesses will go out of business in a short time following a disaster."

Here's a typical scenario. A business might have a small server that stores files that are shared and possibly some virtualised applications. There will be a couple of computers, some tablets and smartphones, and potentially a cloud-based application for customer relationship management of the accounts. Data is spread between multiple devices with some managed within the business and some by external service providers. And locally managed servers are no longer single purpose with virtualisation increasingly common.

SMBs in Australia have one of the highest take-ups of virtualisation in the world with the penetration running at around 25% according to a recent survey undertaken by Symantec. While many similar surveys carried out around the world point to cost savings as the primary motivation for virtualising infrastructure, in Australia the focus is on business continuity and improving server management. But SMBs are looking at cloud and virtual infrastructure as a new platform to make them more competitive in a fast-moving world.

"SMBs are looking at virtualising their backups. With Australia having one of the highest take-

ups of virtualisation it's a fairly important thing to be thinking about but it's often one of the last things considered, much like an insurance policy," says Reeman.

With the opportunities and benefits delivered through the cloud and virtualisation come some challenges. More than 40% of respondents to Symantec's research say they have lost data in the cloud and have had to restore their information from backups. Two-thirds of those organisations saw recovery operations fail.

The trouble is that backup is one of the last things considered. Rather than being part of the system plan from the start, it's seen as an afterthought.

## Planning your backup strategy

In order for a backup and recovery strategy to align with your business needs, you need to do some planning.

You might think that part of what you get when you outsource something to a cloud provider is backups of all your data. Don't rely on the cloud provider to deliver those services. Some do but a lot don't. You still have to think about protecting your data and the sensitivity of that data.

Reeman said, "For backups to be effective you need to plan well, think strategically and think about the protection levels and their appropriateness within the data. Should you encrypt? And review your DR strategy. If you're putting your information in the cloud but you're not backing it up it might not be safe. Cloud providers can suffer disasters just like you can."

When you choose a cloud provider to deliver infrastructure or applications look into their backup plans. Do they back your data up regularly? Is there a cost associated with data recovery? What if the provider suffers some sort of catastrophe? When Amazon Web Services recently suffered outages, their customers - some who were very large - were severely affected.

"What SMBs have to think about is that if they're thinking about moving to the cloud, don't rely on the cloud provider to provide backup services for you. Some do but a lot don't," added Reeman.

Even if there are financial and other penalties in place, should your provider lose data that will be of little comfort if you go out of business.

You also need to contend with increasing mobility and access to so many free and cheap services that are making the landscape of what needs to be looked after more complex. Users are storing data on smartphones and tablets, and using services like Dropbox for personal and corporate information.

Is that data safe? Have you had a 'Scooby Doo moment' when everyone looks around and shrugs their shoulders wondering whether the questions about backup and security have been asked and adequately answered?

For all your systems and infrastructure you need to do an audit. If the accounting system went down, what would be the effects if you couldn't recover all the invoices or orders? Ask the same sorts of questions with every system you use.

Then prioritise the core systems for the business and consider the cost of losing them. This will help prioritise what needs the most immediate attention and help you come to understand the value of a backup and recovery solution.

Look for and clean up duplicated data and consider archiving data that is no longer used. There's little point backing up 10 copies for the same file. Fortunately, many backup tools such as Symantec's Backup Exec can detect and manage part of this through data deduplication technology so that only one copy of the file is kept.

Once you've completed this review, it's time to consider some solutions.

## Choosing solutions

SMBs don't usually have the expertise or time to manage complex systems. They are looking for set-and-forget systems that are reliable. However, you also need to ensure that your backups satisfy a couple of important rules. They need to be stored off-site and you need to test them.

Symantec's Backup Exec can back up data whether it's in a virtual environment or physical. The products are easy to use and cost-effective - everything an SMB is looking for.

There are three versions of Symantec Backup Exec, each offering a different set of features. That means it's easy to choose a solution that matches your needs and financial constraints.

A full matrix of the options can be found at www.symantec.com/small-business/page.jsp?id=compare-backup-exec-products.

# The threat matrix

*Anthony Caruana*

Security is always high up on the list of issues IT decision-makers need to manage. One of the most challenging aspects of security is that the types of threats are changing and the environment we're protecting is shifting as mobility, the cloud and other trends alter the way we work. Anthony Caruana spoke with three security gurus to get their views on the changing threat matrix.

## What is the biggest change to the types of security threats enterprises face?

All three of our panel agreed that the types of threat have changed but each pointed to a different threat. Patrick Gray, security analyst, producer and presenter, Risky Business podcast, said, "The whole concept of APT (state sponsored malware) attacks has really become mainstream over the last few years. The funny thing is, APT-style attacks are nothing new, it's more that awareness of this type of threat has grown."

According to Craig Searle, operations director, BAE Systems Detica, "The single biggest change in the threat landscape has been the movement from mass-produced scattergun-style spam, phishing and defacement campaigns to highly customised and sophisticated attacks." Coupled with Check Point Software Technologies MD Scott McKinnel's identification that, "The biggest change has been the increase in mobile devices being used in the work environment and the breakdown between their owners (staff) and corporate IT." We learn that what worked last year may not work this year and may not even work next year.

## Can enterprises adapt their existing security models to deal with BYOD?

It's obvious that there is no way to eliminate all the risks to a business. However, McKinnel said that "it's a question of educating people and teams within an organisation about how to protect both their devices and the information stored on them".

This is the challenge for businesses and securing their IT environments. The very idea of the organisation's perimeter is far less defined than it was.

Gray said, "The transition to BYOD is really driving some new thinking among smarter enterprises. They're realising it's a chance to really embrace deperimeterisation - they're now able to set up their networks in a way that treats each endpoint with less trust. So when BYOD is done right, the entire network can benefit. When it's done wrong, it's potentially very risky."

Security systems are only as strong as the weakest link in the chain. Searle told us, "Attackers will quickly identify the weakest link within a target organisation and pursue them relentlessly until they have achieved their goals."

## What emerging threats do you anticipate for the coming year?

This is perhaps the most critical question - what's next?

McKinnel said, "Emerging threats include DDoS, botnets and multivector threats. There will be more activism, hactivism, state-sponsored espionage and cyber warfare." Gray was more pessimistic.

"Well, there are two things that concern me - the erosion of the effectiveness of two-factor authentication and the rising popularity of social engineering among a class of attackers who previously haven't presented much of a threat."

Gray sees 'man in the middle' attacks, where authentication information is captured between the sender and receiver. He pointed to recent attacks using malware called Zeus, used to intercept the one-time passwords sent by SMS that are used in banking transfers. "A crew hitting European banks got away with something like $47m doing this," according to Gray.

What was clear in speaking with all three panellists was that the factor to consider when looking at emerging threats was the motivation of the attackers.

Searle said: "Attackers may not directly attack an organisation, instead they attack the underlying supply chain who may not have the same level of security maturity. By compromising these organisations an attacker can quickly abuse the trust relationships between supplier and customer and achieve their aims."

Further to that, Searle also noted that traditional security by logical or physical separation may no longer be enough. "SCADA environments are becoming more commonly targeted, particularly in cases of espionage. Often SCADA environments rely on 'security through obscurity' and operate on dedicated networks that are physically separate from the rest of the corporate environment."

Gray expects to see the collapse of existing authentication methods and shift away from static data, such as birthdays, addresses and the like, when validating personal credentials.

"We've seen some miscreants doing some very clever account hijacking by abusing helpdesk process flaws at companies like Apple and Amazon. Google for 'Mat Honan social engineering' to read a horrifying story about that.

"Authentication headaches are going to grow in 2013 and hit fever pitch in 2015. It's a really awful problem that might necessitate a move to single-use transaction devices, like a tablet computer issued by your bank that can only connect to the bank and nowhere else. I think we'll see this for high-value corporate accounts some time in 2014. They'll stay in use until we can think of a better solution," Gray added.

## Have businesses adapted their thinking around security in the cloud and BYOD world?

While the cloud has become a significant planning and execution concern for enterprise IT departments, it seems that businesses are being slow to adapt their security models for this new paradigm.

Gray says that there's a source of local advice. "One organisation providing stellar advice when it comes to both cloud computing and the BYOD phenomenon is Australia's very own Defence Signals Directorate. They issue edicts to government about these topics and release guidance to the private sector. DSD's work in this area is well worth a look."

"Largely the core model for effective IT security management - Prepare, Protect, Respond & Monitor - remains unchanged," according to Searle. "What has changed is the focus of the individual principles and the level of exposure that non-IT staff have to these principles."

Searle says that IT's role in security is changing as back office teams like finance or HR are now involved in addressing IT security risks. "In today's environment, every single team member within the enterprise has a critical role to play."

## What does "security done well" look like in an enterprise?

We have a theory. When security is done well it's like the umpire at your favourite sporting event. You know it's there but it's not noticeable. McKinnel says that it starts with the C-suite by "having someone in a senior position, such as a CISO".

Similarly, Searle says, "Security done well could be most easily described as having security built into the very DNA of an organisation. Every business process, every job function, every requirements specification would have information security built in as a key consideration. Security becomes part of the culture of an organisation, not dissimilar to antidiscrimination or OH&S."

Gray, on the other hand, hasn't yet seen security done well. "Show me an enterprise that does security well and I'll show you a unicorn that pisses beer." ■

# Four simple steps to build a successful disaster recovery plan

Running a small-to-medium business (SMB) is no easy task. While focused on the day-to-day activities that make your business run - whether it's closing a sale or building the latest widget - having to worry about the bad things that can happen to your business is probably not a preference. But the reality is that something as simple as a deleted or lost file can result in several lost hours of productivity or even the loss of your best customer.

Larger issues can occur from something as innocent as a coffee spill in the server room or a security hack to your network. In less than a heartbeat, your entire network can go down and take your business with it.

If disaster does strike, you simply can't afford to be caught off guard. When critical systems are down or your teams have limited access, the 'bad things' can begin to spiral out of control within minutes. Revenue drops, credibility declines, partners lose trust and a small glitch can escalate into a serious business and financial disaster.

The scary truth is that 74% of SMBs don't have a disaster recovery plan in place. To avoid frightening consequences, every company needs a disaster recovery (DR) plan in place. Why? Because even though you never plan to fail, failing to plan ends with the same bad result. Hopefully you'll never need to go into recovery mode, but if so, you'll be glad you had a plan in place. Although no magic wands can guarantee you're prepared, creating an effective DR plan can be simplified into four easy steps.

## Step one: assess your current situation

Take an inventory of your assets. This includes hardware, software and personnel. Hardware consists of mobile devices, PCs, servers, printers and other physical equipment. Also, take an inventory of the software you have, from your desktop applications to specialised software for sales teams (databases) and engineers. Are any of these proprietary? If so, then they're even harder to replace. Finally, account for all your personnel - who are they and where are they?

Once you have a complete list, you'll need to prioritise what you need to have up and running first, second, third and so on. Think about which apps and files take precedence. Pay close attention to your databases as they contain customer info and are usually most critical to your success. Also, determine which employees need to get back online first. For example, you likely rely on email to communicate. If a Microsoft Active Directory server goes down, then no one can log in. Even if every other system is running, your employees won't be able to use them.

Now that you've prioritised what needs to be up and running first, you need to make an honest assessment of how much productivity and revenue you'll lose from downtime. In a typical outage, SMB customers reported that 52% lost productivity, 32% lost data and 29% lost revenue.[1] Figure out what the likely risks are for you and which risks are unlikely but still possible. There can be physical risks, such as earthquakes, fire, flood and other natural disasters.

There can also be computer-related risks, such as viruses, fraud or security breaches. Last but not least, there are human errors, such as accidental deletion, lost laptops and phones, etc.

When assessing your situation, you'll also want to create a preliminary budget. Keep in mind that when solving for disaster preparedness, you may be able to enable newfound efficiencies. These savings can offset short-term expenses while delivering a long-term return on investment (ROI).

## Step two: define your plan

Next, you'll need to decide what can be done, and when it needs to be done, whether in three months, six months, 12 months or several years down the road.

- Within the first three months, you should have your plan defined, evangelised to your employees (they're the most important part of your business and key to the success of your plan) and budgets allocated - or at least outlined. Take action to implement the initial steps of your plan, such as solving for quick file restore and security plans for lost/stolen devices.
- Within six months you should have your plan implemented. It's imperative to reach the first- and second-tier goals you have for recovery and availability, such as having all employees able have access to data within 30 minutes of a disaster, etc.
- Within 12 months, you should expand your solution for the worst-case scenarios (such as a fire or flood that affects your main office) so you can run from a remote site or get access to your data in the cloud.
- Finally, think two to five years down the road. Take into account where you think your business will be and what you'll need. Will your firm be twice as large? Will new technology change how you access IT?

## Step three: implement your plan

Now, deploy your plan. Depending on the size and scope of your strategy, you may be able to do it yourself or with your existing IT staff. Or you may need help from outside sources. If you already have a trusted partner, they can assist you at major junctions. If not, Symantec can help recommend a local partner with trusted experience.

While implementing your plan, be sure to keep a close eye on your ROI goals. Also, ensure you can meet your recovery point objectives (RPOs) and recovery time objectives (RTOs), too. Be aware that key technologies like virtualisation can greatly increase the flexibility for your business, but can also come with a performance cost. Virtualising correctly not only helps with deploying an effective DR plan, it can help deliver key efficiencies and reduce the costs of running your business. You also need to leverage key technologies, such as comprehensive backup and recovery for all your data.

Keep in mind that when virtualising, you are moving from a more sequential environment, where data requests (from your servers to user desktops) are usually sequential (one after another), whereas in a virtualised environment, these requests are more random. This can result in a performance bottleneck, not too unlike a dozen people trying to get through the same door. For this reason, most companies do not virtualise all of their applications. Many databases, email, web services and other performance or mission critical apps are often kept on physical servers. As such, you should consider a backup and recovery solution that can service physical or virtual machines, as this can be critical to your recovery, simplify management and dramatically lower costs. One solution that meets or exceeds all best practices recommended by industry experts is Symantec Backup Exec, and for virtualised environments, Backup Exec V-Ray Edition (or Backup Exec virtualisation agents for current users). These full-featured solutions deliver leading performance, the flexibility to restore critical files quickly and easily, as well as the ability to restore entire virtual or physical servers (even to different hardware).

One more important point: Be sure you clearly define what will make your plan a success. This includes outlining clear and measurable recovery points and quality of functionality.

## Step four: reassess your plan

Last but not least, test what you have in place to see if you're meeting all targets for ROI, RPO and RTO. The ability to test without shutting down your production environment, along with automated failover, should be a key end goal. By starting early, you can adjust as needed in all areas.

## Summary: be proactive, begin your disaster recovery plan today

You never expect a disaster to happen. But if and when it does, you can save your company critical time, dollars and effort if you're 100% prepared. To put it bluntly, you can also save your company. Consider this: 43% of companies that experience a disaster never reopen, and 29% shut their doors within two years.[2] Those are telling numbers on the importance of a disaster recovery plan.

Of course, no two businesses are the same, and your disaster recovery plan should be as unique as your company. However, by following these four simple steps, customised to fit your situation, you'll be well prepared should a disaster strike. If you need help creating your disaster recovery plan, be sure to contact your Symantec representative for more best practices and advice.

1. *Symantec 2012 SMB Disaster Preparedness Survey Global Results, May 2012*
2. *Mel Gosling & Andrew Hiles "Business continuity statistics: where myth meets fact", Continuity Central (24 April 2009), http://www.continuitycentral.com/feature0660.html*

# Finding the perfect fit

## Backup and recovery for virtualised environments

### Introduction: calling for backup

Every business needs to:

- Protect critical data and systems against costly downtime by ensuring effective backup and recovery are in place.
- Consider the cost and efficiency benefits that can accrue from a switch to wholly or partly virtualised IT environments.

But do the two mix?

Whether it's reductions in hardware costs and space requirements or the ability to keep pace more easily with data growth, the appeal of virtualisation is obvious - especially for smaller companies, now outstripping larger organisations as adopters.[1] A recent TechTarget survey revealed that the average small- to medium-sized business (SMB) in Australia and New Zealand has virtualised 54% of its servers.[2] But virtualisation brings challenges too, not least the threat to business continuity, compliance and reputation if data on virtual machines (VMs) isn't backed up properly and systems can't be recovered rapidly whenever they go down.

With no shortage of vendors offering solutions, the market has become a jungle overgrown with confusing and conflicting claims and counter-claims. So how can you leverage the right solution for your organisation, your needs and your virtualisation strategy?

Helping you identify the option that's the perfect fit for your requirements, this article aims to ensure that concerns over backup and recovery don't deter or derail your efforts to exploit virtualisation and its undoubted business benefits.

### Virtual views

Virtualisation isn't a 'one size fits all' phenomenon. Each individual business will have its own view of how it can harness virtualisation and the extent and pace at which it should do so. Although around 20%[3] of organisations currently plan to maintain physical-only IT environments, the rest fall broadly into three different categories:

#### *Converting (56% of organisations)*

Businesses either taking, or about to take, their first steps away from a purely physical IT environment and towards a virtual or hybrid physical/virtual one. Such a step may involve, for example, installing a number of VMs on one physical server.

#### *Embracing (24% of organisations)*

Businesses that have set up, or are in the process of putting in place, a highly virtualised environment.

For these organisations, it will be vital to ensure that all key elements of their IT ecosystem (eg, backup and recovery) keep pace with this evolution.

### *Rationalising (a subset of 'Embracing')*

These businesses have moved towards virtualisation but have incrementally introduced a variety of backup, recovery and other components perhaps sourced from a range of vendors, and now want to rationalise them to cut the complexity and cost of operation, management and admin.

Consistent with this differentiation, backup and recovery for virtualised environments isn't a question of 'one size fits all' either. It's about finding a solution that has the ability to provide the right level of protection for your organisation, depending on which of the three categories you fall into. Unfortunately, getting this key decision wrong could mean making a very expensive mistake: a 'solution' that delivers less than you need will inevitably leave your business vulnerable, while a solution that delivers more than you need could mean incurring unnecessary costs.

So how can you avoid these dangers and make the right call?

## Sound solutions?

For SMBs, in particular, developing and maintaining effective backup and recovery capabilities purely in-house, with all the associated capex, opex and staff time implications, just isn't viable. Buying in a third-party solution for your virtualised environment is the only practical course of action.

But even the most cursory internet research reveals a big problem: a blizzard of different vendors stating they're 'number 1 for VMware backup' and often supporting this confident assertion with questionable claims that are completely unsubstantiated or based on unscientific 'tests' or 'surveys'.

Who to believe?

When attempting to wade through the flood of competing offerings, it's absolutely vital to be clear over the backup and recovery 'must haves' that any organisation needs when it opts for virtualisation. The 'Big Six' are:

### *1. Common backup platform*

As well as boosting admin efficiency, unified backup across virtual and physical environments (supporting both physical servers and multi-hypervisors/virtual machine monitors) is essential to ensuring comprehensive protection of data, applications and systems.

### *2. Comprehensive data deduplication*

Dedupe needs to span your entire IT environment, virtualised and physical, in order to minimise the amount of data requiring backup and thus reduce not just backup windows but also storage costs.

### *3. Total data integrity*

All data needs to be secure, robust and tamper-free at every single stage of the backup process, to ensure full functionality and robust regulatory compliance too.

### *4. Reliable, rapid, granular recovery*

To minimise business downtime, full data and system recovery needs to take minutes, not hours. Solutions should also enable recovery of everything down to single files or emails, whose immediate availability could be vital to time-critical actions such as submitting a tender or successfully exploiting a sales lead.

### *5. Scalability and integration*

Backup and recovery solutions need to be capable of organic growth as your business and data loads expand. Meeting growing needs by adding point solutions on a multi-vendor basis will inevitably lead to management inefficiencies and could also create vulnerabilities because solutions don't dovetail together properly.

### *6. Transparent costs, affordable price*

All too often, a low headline price won't translate into low total cost of ownership (TCO). For instance, TCO will just keep racking up if the solutions you choose:

- Can't retrieve granular items, making it necessary to perform time-consuming manual searches.
- Don't dedupe effectively and comprehensively, inflating your storage costs.
- Won't deliver the recovery speed needed to protect against downtime and the bottom line losses that can result.

## Right to choose

In virtualised environments, your business can only stay sure and secure if backup and recovery capabilities aren't compromised. And that means pinpointing a backup and recovery vendor who unambiguously offers:

- The proven capacity to protect you effectively (and indeed cost-effectively), in line with the Big Six above.
- A suite of different offerings specifically geared to meeting different types of need, depending on whether your organisation is 'Converting', 'Embracing' or 'Rationalising'.

When making the right choice, then, it's vital to identify hard facts and penetrate the marketing hype. In reality, only one vendor:

- Can claim 40% market share in VM backup and recovery, based on global revenue.
- Offers a portfolio of products matching different needs, delivering the 'must haves' outlined earlier and building on a track record acquired in some of the most demanding IT environments in the world.

The table below outlines three key products from Symantec's industry-leading suite of backup and recovery solutions, designed to provide benchmark capabilities and performance across wholly or partially virtualised environments:

| Your Business's Virtualisation Status | Symantec Solution | In summary |
|---|---|---|
| Converting | System Recovery 2013 Virtual Edition | A backup and recovery solution that protects one physical server hosting several VMs, enabling recovery from downtime and disasters in minutes. |
| Embracing | Backup Exec 2012 V-Ray Edition | Designed for highly virtualised environments and licensed per occupied processor socket, this solution protects an unlimited number of guest machines - simplifying the complexity of hypervisor protection, reducing backup windows and providing fast restoration of an entire VM through a single-pass backup. |
| Rationalising | Backup Exec 3600 Appliance | Licensed per appliance4 and designed to provide optimum licensing simplicity, this total, all-in-one 'best backup in a box' solution integrates software and hardware and protects physical and virtual servers, applications and databases, while ensuring simplified setup and management. |

## Suite success

Centralising workflows across all your platforms, this Symantec suite of solutions provides the confidence you need to exploit virtualisation, safe in the knowledge that this won't mean compromising on backup and recovery. Every feature is individually and collectively designed and calibrated to maximise effectiveness and minimise risk:

| Product | Key Features |
|---|---|
| Symantec System Recovery 2013 Virtual Edition | • Restore Anyware™ technology, enabling rapid restoration of precisely what you need, when and where you need it.<br>• Cross-platform physical to virtual, virtual to physical and virtual to virtual recoveries. |
| Backup Exec 2012 V -Ray Edition | • V-Ray technology sees right across your entire IT environment, resulting in a comprehensive cross-platform solution.<br>• Provides bare-metal and granular recovery.<br>• Each licence includes: Backup Exec 2012 media server licence;agent for applications and databases to protect unlimited number of virtual guests; agent for VMware and Hyper-V; dedupe option.<br>• Backup environment can be customised by adding further agents and options. |
| Backup Exec 3600 Appliance | • The appliance includes: Backup Exec 2012 software; dedupe option; agent for VMware and Hyper-V; agent for Windows; agent for applications and databases; remote agent for Linux; remote agent for Mac |

Success in business means making the right calls. In the age of virtualisation, picking a data backup and system recovery solution that combines proven effectiveness with low TCO really is a 'must have' that can equip you to enhance efficiency, cut costs and sharpen your competitive edge.

With Symantec solutions, virtualisation and cost-effective backup and recovery do mix.

1. *eg http://www.symantec.com/connect/blogs/virtual-visibility-why-you-need-x-ray-vision-backup-virtual-machines.*
2. *'Server Virtualisation Gains Mometum in Small Businesses, but Backup Adoption for Virtual Machines Still Lags': survey commissioned by Symantec and conducted in January 2013.*
3. *This percentage and the subsequent two figures are based on findings from the previously cited TechTarget survey.*
4. *One appliance protects up to 5.5 terabytes of deduped data.* ■

# resources

## from our sponsor

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world.

www.symantec.com.au
1800 000 423

**Symantec Internet Security Threat Report, Volume 18:**
http://go.symantec.com/istr

**Solutions for Physical and Virtualised IT Environments, A Guide for Small to Medium Businesses:**
www.symantec-smb-solutions.com/au/backup/pc-or-server-backup.aspx

**The Rise of Ransomware – How to protect your Business:**
http://www.symantec-smb-solutions.com/au/resources/whitepapers/how%20to%20stop%20your%20business%20being%20taken%20hostage/register.aspx

**Symantec Small to Medium Businesses Solution Centre:**
www.symantec-smb-solutions.com/au/

wf online
a division of Westwick-Farrow Media

food processing .com.au
Food processing, packaging & design

labonline .com.au
Life, analytical & environmental science

processonline .com.au
Automation, control & instrumentation

radiocomms .com.au
Professional radio communications

electronics online.net.au
Professional electronics design & engineering

safety solutions .net.au
Industrial, construction & mining safety

sustainability matters .net.au
Solutions for industry & government

ECD SOLUTIONS
www.ECDsolutions.com.au

technology Decisions
www.technologydecisions.com.au

Australian LifeScientist
www.lifescientist.com.au