VERITAS

The truth in information.

How Ransomware ready are you?

BE sure your physical, virtual, and cloud data doesn't fall victim. Just BE.

The concurrent execution of 'Wannacry' extortion attacks across the globe in May 17 served as a dramatic reminder of the dangers out there in the cyber sphere.

Although these attacks saw high-profile organisations like FedEx and the UK's National Health Service making the biggest headlines, they also took their toll on a large number of other businesses, causing widespread disruption, interrupting services, and locking down files.

In light of those issues, of countless other emerging ransomware threats, and of the resulting cyber readiness report from Hiscox containing data commissioned from Forrester, this ebook asks a key question: What can companies – especially smaller companies – now be doing to ensure they are protected and shift from 'cyber novices' to 'cyber experts'?

Accordingly, here we review the landscape and the simple cost-effective measures companies can take to protect their physical, virtual, and cloud-based data. Today.

> What is ransomware? Malware that locks up valuable data and demands that businesses or individuals pay for decryption keys to release it.

Ransomware crime is on the rise

The Wannacry attacks were simply one example of ransomware's rapidly escalating threat. With a 6000% increase in attacks in 2016 alone[1], it is already a billion-dollar business. Worse still, incidents are forecast to double through 2017[2]. And organisations both large and small are likely to be on the frontline.

> *"If the events of the WannaCry incident are anything to go by, we may be about to see a significant uptick in the continued rise of ransomware."*[3]

What's at stake?

As well as the immediate fallout of an attack, such as financial loss and interrupted business, Hiscox points out that companies need to consider longer-term "ripple effects", including damage to reputation and client relationships.

There's also the small matter of the ransom fees themselves – with reports of companies paying six-figure sums to unlock their data – not to mention the increased likelihood of a second extortion attempt[3].

72% of large US firms reported a cyber incident in the past year[4]

32% lose data access for 5 days or more[5]

20% of victims who pay a ransom don't get their files decrypted[6]

Who's at risk?

The short answer? Everyone. Half of all US companies have been affected by ransomware over the last year[3]. High on this list were business services, construction, property, technology and telecoms firms. But the fact is that virtually any business with valuable intellectual property is a potential target. That includes law firms, accountants, hedge funds and brokers – and countless others.

[1] WSJ Pro Cybersecurity report: the WannaCry Cyberattacks: Dealing with the Risks, 2017 [2] Beazley Breach Insights, January 2017 [3] WSJ Pro Cybersecurity report [4] Hiscox Cyber Readiness Report 2017, with data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox. [5] Symantec ISTR Special Report: Ransomware and Businesses 2016 [6] Intermedia Ransomware 101: What your business needs to know about ransomware attacks, March 2016

Smallest firms hit the hardest

The financial impact of cyber incidents tends to be disproportionately higher for smaller companies. A small business in Germany might pay up to 48% of what an organisation ten times its size would pay[4].

Small, and even medium-sized businesses are also less likely to be prepared, and so attract more attention from cyber criminals. Unfortunately, it turns out that such companies also seem to be the most complacent, with 29% made no changes at all following cyber security incidents. This is particularly worrying given that, to reiterate, a company is statistically much more likely to be attacked if it has already fallen victim.

> *In relative terms, small companies are paying the highest price for operating online.[8]*

Cyber readiness model: More than half of firms are 'novices'

Forrester's cyber readiness model rates firms as 'cyber experts', 'cyber opportunists' or 'cyber novices' according to how well defended they are against cyberattacks and incidents. Just 30% of those surveyed were 'experts', while more than half turned out to be novices. Clearly there is a large gap, and it needs to be closed.

53%
of companies are 'cyber novices[8]'

49%
of 'cyber experts' were in the US[8]

85%
of 'cyber experts' say faster response times is a top priority[8]

[8] Hiscox Cyber Readiness Report 2017, with data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

A simple solution. Backup your data.

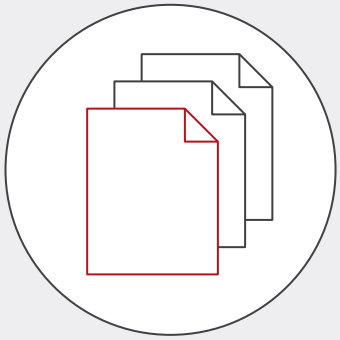
While anti-virus software is an essential component when it comes to looking after your data, it's no guarantee whatsoever when it comes to ransomware. But, implemented and maintained properly, a robust backup strategy is.

You just need to BE backing up in the right way.

So here are the **5 key measures** every business should BE taking to protect themselves and start becoming cyber experts

1

Copy it

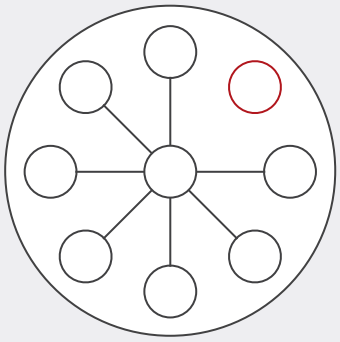


If it's only backed up once, it's not backed up. Twice is okay. Three times is a charm.

With **Backup Exec** it's easy to extend the automation of secondary storage – including **Microsoft Azure, Amazon Web Services and Google Cloud** – for enhanced protection and recoverability. It creates a single backup job that supports migrating backup data from expensive primary disk storage to cheaper secondary disk or cloud storage, disk-to-disk-to-tape backup, and more.

2

Isolate it



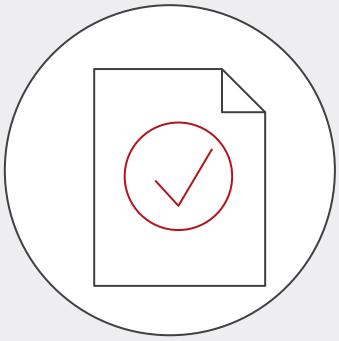
Keeping backup copies of your data off site will provide an extra level of safety. Ensuring removable media like tape is stored remotely or using cloud storage will place a further isolation layer between ransomware and your backup copies.

In addition, **BE** sure your backup destinations can be accessed by Backup Exec servers and nothing else. **That way they can't be compromised by intruders.**

Backup Exec has one of the industry's most comprehensive compatibility lists, with direct integration for writing data directly, quickly and reliably to public cloud and removable media, preventing the secondary infections that affects disk-based-only protection.

3

Keep it



Retain your backups. ALL of them. Even in the event you're compromised but you think you've recovered. If your backup strategy does not include a retention scheme that preserves multiple copies of your data you could end up overwriting a good backup with encrypted or 'dirty' data, so you can't be too careful.

Backup Exec enforces and automates the retention of multiple backup copies wherever necessary. So whatever your choice of storage, **you're protected for the long term.**

It also offers the ability to retain backup copies indefinitely. So in the event ransomware should be detected in your environment, placing a hold on your backup copies helps ensure prior backups can't be overwritten.

4

Back it up. Frequently.

BE sure to backup not just frequently, but regularly enough to meet your recovery point objectives. BE sure to review your jobs and schedules to verify that your backup frequency provides protection in line with your objectives.

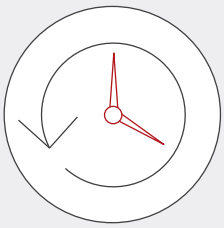
To reiterate, make sure you're backing up to multiple destinations. A useful rule of thumb here is the 3-2-1 guideline – Back up to **three** different destinations, using at least **two** different types of media, storing at least **one** copy offsite.

Again, if possible, allow your backup destinations to be accessible only by Backup Exec media servers and no other systems. Backup Exec has a broad set of options for secondary storage, including cloud storage services offered by Amazon Web Services, Microsoft Azure, and Google Cloud. See the Backup Exec Hardware Compatibility List for all of the supported options.

Backup Exec Instant Granular Recovery Technology™ (GRT) accelerates this process allowing single file, folder, mailbox, or database object recovery.

5

Test it



Everything's in place, but will it work? You should ensure the correctness of your backups and test your Bare Metal Restore™ responsesand overall ability to recover from ransomware attacks on a regular basis.

You can do this by using the Backup Exec Simplified Disaster Recovery, automated recoverability verification, and Recovery Ready features.

3-2-1 Go!

Don't forget the 3-2-1 rule of backup

3 backup destinations

2 kinds of backup media

1 offsite copy. At least.

> *Data backups are one of the most critical pieces of defensive strategy against ransomware.*[3]

We have some fantastic time-limited special offers too. So get unified backup with Veritas.

The timing – and the savings – couldn't BE better.

Save today