SMB

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

Small and Midsize Businesses: Rip the Target Off Your Backs

Debunking the top five myths about ransomware and SMBs

Introduction

SMBs have limited time and IT resources, and a lot on their plates – especially when it comes to cybersecurity. Unfortunately, SMBs have become the biggest target for ransomware attacks, and they need to face the harsh truth that ransomware can wreak havoc with data, budget and reputation.

In a typical ransomware scenario, the SMB receives a warning that critical data has been encrypted and the organization will need to pay a ransom to get the decryption keys. If the company decides to pay the ransom, there's no guarantee the keys will be provided; an unfortunate 15% report that even after transferring the payment their data is not decrypted [i]. Even if they do manage to decrypt the data, they are likely to be hit again and again.

Those companies that refuse to pay the ransom may find themselves victim of a new, insidious threat: the attackers will steal a copy of the data, then threaten to sell it on the dark web. Should this happen, the company could be subject to steep fines if it fails to notify authorities in a timely manner, as required by GDPR and similar regulations, not to mention the potential damage to the company's brand and reputation. And, again, just because the company was hit once doesn't guarantee it won't be attacked again.

Yet many SMBs are not aware of the risk they face. This paper will debunk the most common myths surrounding ransomware, and present ways to help prevent ransomware attacks, protect data and ensure an adequate recovery procedure.

i https://www.securitymagazine.com/articles/90316-ransomware-is-the-biggest-threat-to-small-to-medium-businesses

Myth 1

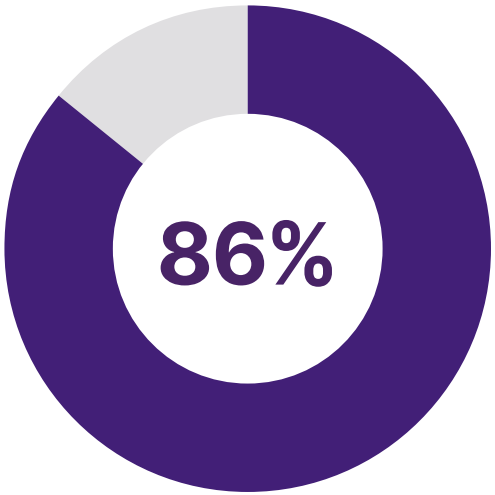
My company is too small for attackers to bother with

Today it's not just the large organizations that are being hit. Almost anyone is a target for ransomware. In fact, SMBs represent an increasingly attractive target for attackers: According to one global report, 86% of SMBs reported they had been victimized by ransomware – and more than 20% of them were hit six[ii] or more times. In fact, small businesses suffer close to 10,000 cyberattacks daily[iii].

In a way it's even more serious when a small organization is hit. While large organizations often have robust security teams and big budgets for multiple layers of defense, SMBs often rely on very small teams or a single person for planning, coordinating and leading all IT-related activities. Security is piled on top of all the other day-to-day activities. The recent move toward remote working only increases the threats. More workers than ever are using RDP (Microsoft Remote Desktop) to access their work desktop, and setting it up using default settings can allow criminals to do brute-force attacks, gaining access to corporate resources. For SMBs, these types of issues can increase the attack surface area as many extremely important issues remain unaddressed. Planning for dealing with ransomware is too often one of these issues.

Yet ransomware is not going away, and it's getting more costly for SMBs. Where a year ago the cost averaged $34,000, today it has risen to just under $200,000[iv].

"[Ransomware] is a big problem that is getting bigger, and the data indicates a lack of protection from this type of malware in organizations.[v]"



of SMBs reported they had been victimized by ransomware[ii]

ii https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf
iii https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html
iv https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
v https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Myth 2

There's no way to prepare for a ransomware attack

While ransomware attacks may seem to be inevitable, there is much an SMB can do. The key is reducing the likelihood of an attack, and making sure critical data is protected in case an attack succeeds.

Defend against ransomware attacks

The way ransomware gets into an organization is often by tricking a user into downloading a file with macros that run automatically (the recent Emotet and Trickbot attacks scanned the environment and allowed criminals to determine if valuable data is present), then download a ransomware payload such as Ryuk.

Webroot provides several ways to stop this from happening. Webroot® Evasion Shield, part of Webroot® Business Endpoint Protection, automatically stops malicious macros from running. Webroot Business Endpoint Protection prevents the user from downloading malicious payload from known bad URLs and IP addresses, and it can analyze files before they are executed to determine if they show malicious intent or behavior. Reliable endpoint security is a must for SMBs, especially since attackers are constantly finding new ways to attack.

Protect your data

Data is the lifeblood of an organization; losing access to it can cause serious damage. Backups are vital. However, performing lengthy full-server backups (which take time, resources and network bandwidth) or relying on end users to do their own data backups (seldom a priority and often forgotten) are not optimal solutions. Instead, there are several better ways to protect data.

Carbonite® Endpoint automatically protects endpoints and their data, while Carbonite® Server backs up data from physical and virtual servers. For data on older servers that are running operating systems no longer supported, SMBs can move the data to a more protected environment via Carbonite® Migrate, and then back up the data automatically using Carbonite Server. These solutions are efficient since they only back up data that has changed once the initial process is complete. And, they are safe – SOC 2 certified, and support compliance with important regulations such as HIPAA, FERPA, GDPR GLBA and the like.

A common misbelief is that if the company is using Microsoft 365, OneDrive or DropBox, their data is protected. However, ransomware can simply be replicated to the cloud and can even spread from there across networks via shared files and folders. To avoid this, SMBs can use a dedicated backup solution from Carbonite to ensure that all critical data is backed up, consistently, and that backed up copies are protected.

In addition, both Carbonite® Recover and Carbonite® Availability provide fast recovery by failing over to a secondary environment while the virus is wiped from the source. This can help SMBs keep their businesses running during the attack itself.

Don’t forget to protect your backup copies

Local copies make for faster restores, but it’s important to protect the backup itself. This means running it on a separate network, using different credentials, to ensure that in a breach the ransomware won’t spread to the backup itself. Carbonite Professional Services can provide expert assistance to SMBs on how best to configure backups for maximum protection.

Many companies that use cloud-based backup sync services don’t know of an important vulnerability: They are often able to store only a limited number of backups. The attackers will encrypt the files in a synced folder, wait a period of time for those files to be synced to the cloud, then encrypt those files again. It will repeat this process in an attempt to eat up all the previously synced versions of a file with encrypted copies. In this way, cloud sync backups like Google and Microsoft are defeated. Carbonite® Server, in contrast, backs up on a schedule set by the customer, who can also set the minimum number of days before expiring. E.g. if a customer has a one-year retention policy and sets the value to 365, the monthly restore point will not be removed before 365 days.

The Town of Colonie, NY avoided more than $400K in ransom due to backup. Hit with a massive ransomware attack, the IT team immediately checked their three Carbonite Server appliances that had been placed at offsite locations based on guidance from the Carbonite Professional Services team. Finding the backups intact, they disconnected them from the network and were able to start the recovery process, with minimal downtime and data loss – and without paying the ransom.

Myth 3

If I have a backup plan in place, I am safe

Preventing ransomware attacks and backing up critical data are both extremely important proactive measures, but if the worst happens, critical systems and data need to be recovered. There will be some downtime, which can be costly and damaging. It's imperative to recover critical systems and data very quickly, restoring data from safe backups that haven't been infected with the ransomware itself.

While big companies can invest in redundant servers in secondary locations, this can be cost-prohibitive for SMBs. Many of them look to disaster recovery as a service (DRaaS), leveraging the cloud to support greater IT resiliency. Carbonite provides DRaaS for modern cloud and virtual systems – with the added benefit of also covering legacy systems like IBM iSeries and AIX. All data is encrypted, and SLAs are provided for rapid recovery. By continually syncing the recovery systems with primary servers, this ensures that critical business systems are online and accessible, no matter what happens on your network. If an outage happens and a failure threshold is exceeded, the system will immediately fail over to the cloud-based replica.

Here too Carbonite Professional Services can help with, or completely take care of, disaster recovery planning, testing and documentation. The team works with the SMB to perform DR tests prior to activation, to ensure accuracy and efficiency if an outage such as that due to ransomware does occur.

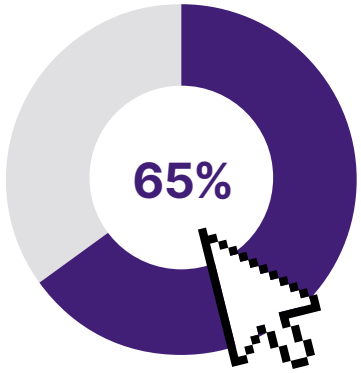
Myth 4

Technology alone will save me

Cyberattacks are not purely a technology problem, and the solution cannot rest entirely on technology. Remember that people are the first line of defense. They can fall prey to a phishing attack, inadvertently click on a dangerous link or download malware that invades the entire network. An astonishing 93% of security breaches start with a phishing attack[iv]. That makes it imperative that users become much more aware of security threats and how to deal with them.

Security awareness training that includes phishing simulations and training in data protection are becoming standard practice for SMBs. It's a proven way to reduce risk, decrease infections and help desk requests, reduce the chances of a security breach and strengthen the overall security posture. Webroot® Security Awareness Training includes engaging, interactive courses that are easy for users to consume but lead to lasting security improvements: Comprehensive training with targeted simulations and continuous, relevant education reduces users' security error rates to 5% or better[vii]. Importantly, phishing simulations are updated often to ensure they correspond to current topics that are used by attackers to entice users to click on links, such as remote working. Regular security awareness training builds up users' "muscle memory" so they stay attuned to malicious attempts and can strengthen the corporate security shield.

Webroot has found that running 11 or more training campaigns over four to six months reduces phishing click-through rates by



iv https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
vii Webroot Security Awareness Training research

Myth 5

It will be hard to get all this to work together seamlessly

Some gaps in security will always remain, but SMBs can strive for cyber resilience: the ability to withstand security attacks and land on your feet, no matter what happens. Cyber resilience protects the business, customers and employees from whatever digital challenges they may face – not just ransomware, but a host of other potential issues.

Cyber resilience from Carbonite and Webroot offers a seamless approach to prevention, detection and recovery. The comprehensive stack of cyber resilience solutions helps keep companies secure and their data protected, so they can continue to serve their customers, employees and investors regardless of the cyber challenges they may face. SMBs use the suite of Carbonite and Webroot solutions to cover the entire range of prevention and recovery options.

Conclusion

It's said that hope is not a strategy. Rather than hoping your business isn't hit with a ransomware attack, or hoping your backups will remain uninfected, or hoping your cloud-based data will be protected, a better approach is to plan and prepare to prevent ransomware and other cyber-attacks. When you take action to better protect your data and plan for recovery in the event of a successful attack, you are one step closer to achieving cyber resiliency.

Contact our experts to find out how data protection is critical to improving your company's cyber resilience.

Contact us to learn more – Webroot US

Phone: +1 800 772 9383

Email: wr-enterprise@opentext.com

Contact us to learn more – Carbonite US

Phone: 877-542-8637

Email: carb-data_protection_sales@opentext.com

i https://www.securitymagazine.com/articles/90316-ransomware-is-the-biggest-threat-to-small-to-medium-businesses
ii https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf
iii https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html
iv https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
v https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
vi Verizon, op. cit.
vii Webroot Security Awareness Training research

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.