WEBROOT®
opentext™ Business Solutions

Guide to Cyber Resilience for MSPs

Learn about:

- Why the SMB needs cyber resilience as much as the enterprise
- What should be part of your cyber resilience strategy and how to take it to market

Powered by ConversationalGeek®

Nick Cavalancia
Microsoft MVP

Brought to you by 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.

CARBONITE® + WEBROOT®

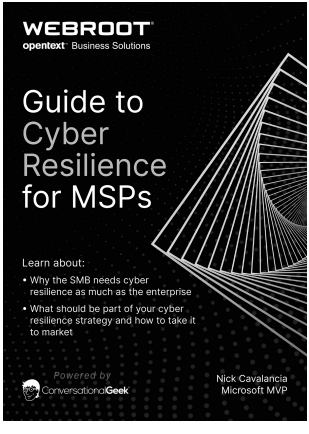
opentext™ Business Solutions

CARBONITE® + WEBROOT®

opentext™ Business Solutions

Guide to Cyber Resilience for MSPs

by Nick Cavalancia



Powered by ConversationalGeek

conversationalgeek.com

Guide to Cyber Resilience for MSPs

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at www.ConversationalGeek.com.

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Nick Cavalancia
Project Editor:	Pete Roythorne
Copy Editor:	Kyle Fiehler
Contributors:	Jennifer Grimaldi
	George Anderson

The “Conversational” Method

We have two objectives when we create a “Conversational” book. First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand Read ’em!

The SMB Needs Cyber Resilience

"Of course we're secure – we have antivirus installed!"

The SMB can no longer think of itself as flying under cybercriminals' radar. The reality today is cybercriminal gangs think like regular reputable businesses, targeting specific industry verticals, geographies, and, yes, sizes of organizations – which includes the SMB.

Today, the SMB is just as much a target of nearly every kind of cyberattack as their enterprise counterparts:

- Data Breaches – SMBs were the victim in 46% of all data breaches, with malware, hacking, and social engineering as the top three threat actions used[1].

- Ransomware – 33% of SMB organizations admit to having been the victim of a ransomware attack in the last 12 months[2].

- Credential Theft – Usernames and Passwords are the number one data type stolen from the SMB[1].

- Business Email Compromise (BEC) – Impersonation and fraud plague every size

---

[1] Verizon, *Data Breach Investigations Report* (2021)

[2] Sophos, *State of Ransomware* (2021)

business but are particularly easy in smaller businesses with less processes and formality with financial transactions.

And it doesn't appear like it's going to be getting any better; 40% of SMBs think the number of cyberattacks has increased over the last 18 months (with only 13% thinking it's decreased)[3]. Despite this, it's far more likely that your prospective SMB customer isn't well prepared either.

The SMB Isn't Ready for an Attack

Today's cybercriminal is incredibly well-versed in how to social engineer, use readily available malicious tools and services, hack into and traverse a victim's network, and knows how to make the most money from their efforts.

You'd think at this point, the SMB owners and operators would be smart enough to see it, but the reality is that SMB's just aren't ready should an

---

[3] Webroot, *Perceptions and Misconceptions on AI and Machine Learning in Cybersecurity Report* (2021)

attack occur. Take a look at the table below and see what percentage of SMBs are taking proper precautions against cyberattacks. According to recent Webroot data[3], SMBs are doing the following:

Regularly backing up company data	51%
Using antivirus or antimalware protection on company devised	50%
Installing software updates on company devises regularly	42%
Requiring employees to use different passwords for each platform/account	37%
Requiring the use of two-factor or multi-factor authentication (2FA/MFA)	33%

Overall, this makes the average SMB look to be rather insecure. In almost every case, less than half of SMBs are doing these *basic* security measures. Backups, patching, endpoint protection, password hygiene – these are baby steps that every business should have in place to protect and prevent (and in

the case of backups, specifically – *respond to*) a cyberattack.

While this isn't entirely surprising, it sort of is, in that, by now you'd think every SMB owner is aware – at least anecdotally – of the repercussions of being a victim of a cyberattack.

The Impact of Cyberattacks on the SMB

Organizations of all sizes within the SMB feel the pain of a cyberattack just as much as an enterprise business. And there are a few tangible impacts they experience:

1) Downtime – Depending on the type and scope of an attack, systems, applications, and data may be unavailable for days, weeks, or months. 57% of SMBs experience downtime after a breach[4].
2) Lost Productivity – With some or all of production out of commission, employees

[4] Sectigo, *State of SMB Security and Threat Report* (2021)

can only do so much work before being sent home. 33% of SMBs experience lost productivity after a breach[4].

3) Loss of Customer Confidence – An SMB's customers depend on them to be up and running, as well as to maintain the security and privacy of any customer, credit card, or personally-identifiable data. When a business fails to meet these expectations, at a minimum, customers need to be reassured an organization has a handle on the situation and that it won't happen again. 39% of SMBs experience a loss of customer confidence after a breach[4].

4) Loss of Customers – Some customers aren't so forgiving after a breach and will go looking for another company to do business with. 33% of SMBs experience a loss of customers[4].

5) Loss of Revenue – All of these impacts culminate in the form of lost revenue, which has obvious repercussions around the viability of a small business that may or

may not be able to sustain itself post-attack. 36% of SMBs experience a loss of revenue after a breach[4].

Just to make the point about the impact of a cyberattack on an SMB from a 50K-foot view, according to *US Telecom's 2021 Cyber Security Survey* of Critical Infrastructure SMBs, on average it takes *7 and a half months* to fully recover from a breach!!!

Without belaboring the point, the SMB simply can't afford to be hit with a cyberattack that takes out their operations for some material amount of time.

What they need is to be cyber resilient.

Even SMBs Should be Cyber Resilient

The statement above requires a bit of definition around what exactly does is mean to be *cyber resilient.* In a general sense, cyber resilience occurs when an organization has an ability to "bounce back" from a cyberattack and quickly return to an operational state that is known to be secure.

The Presidential Policy Directive PPD-21 defines resilience as *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions*. Notice the three verbs used: *adapt*, *withstand*, and *recover*. In an ideal scenario, an SMB should be able to adapt their security measures to align with the current state of cyberattacks *so that* they can withstand an attack (e.g., stop a malicious email from reaching a user's Inbox) or recover from a successful attack (meaning they can regain operations quickly using whatever technical means is necessary, including the literal interpretation of the word *recover*.

The challenge for most SMBs is they don't have a clue on how to achieve this.

That's where you come in.

The MSP Opportunity

Your MSP business exists because a need existed by a customer to outsource their IT to a trusted and experienced partner. Cyber resilience is the next "need." The opportunity exists here to not just

“secure” your customers, but to truly make them resilient in the face of evolving cyberattacks.

Some of you reading this many be completely new to offering any kind of security services, with others having years of security experience. Regardless of your situation, the call here is to first be thinking in terms of resilience, not protection; consider the end goal (to make your customer be able to regain operations quickly in the face of a damaging cyberattack) and work backwards to the services that should be included, continuing backwards to the technology, people, and processes necessary to achieve that goal.

This all sounds great, but I think we need to speak in more practical everyday MSP terms so you can begin to formulate a plan to offer cyber resilience services.

Defining a Cyber Resilience Service

If you stop to think about it, defining a standard service that is going to make certain that every one of your customers – with all their nuances, industry-specific needs, peculiarities, and the occasional one-off configurations – is resilient when attacked is no simple task.

So, let's first define – in practical terms – what exactly does it mean to make your customers *cyber resilient* in order to create a service offering.

Using the previous definition of *resilience*, the goal is to *adapt to*, *withstand*, and *recover from* a cyberattack. So, how does that translate to services. Let's break it down:

Adapt

The *adapt* part defines more an overarching need to ensure whatever solutions are put into play will be able to adjust to the evolving threat landscape. There are two aspects of modern-day solutions you should be looking for to ensure that a) the whole *adapt* aspect of your service gets a big checkbox

next to it and, more importantly, b) you're service automatically adapts without you needing to do anything.

This is accomplished with security solutions that employ two factors:

1) Threat Intelligence-based – There are a large number of both open-source and privately-managed threat intelligence databases today that are updated constantly based on the malware, social engineering tactics, and threat actions of cybercriminals. The solutions you employ must be leveraging one of these to automatically remain up to date with current threat tactics.

2) Use of Machine Learning (ML) – For any given emerging threat, some system somewhere in the world is the first one to see it. So, it's necessary that the solutions you employ also have a level of artificial intelligence (AI) that allows it to see

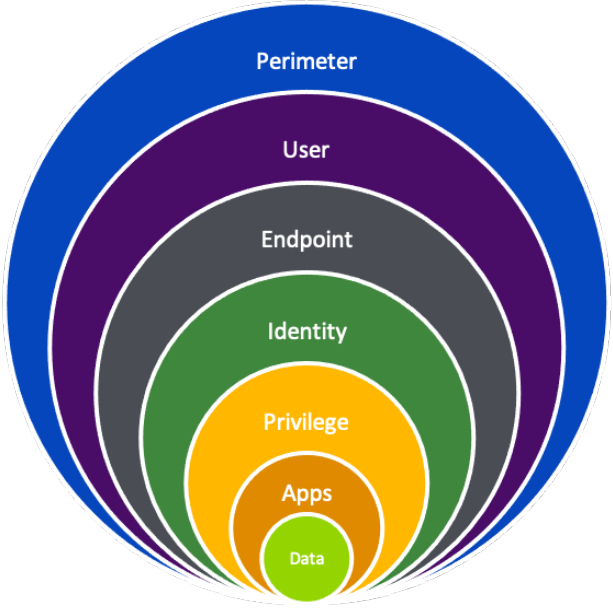
something never-before seen as potentially dangerous.

By current estimates, there is one cyberattack every 11 seconds in 2021. With cybercriminals constantly evolving their tactics to avoid detection, it would be impossible for security solutions to keep up without threat intelligence and AI/ML.

Withstand

The *withstand* speaks to the need to protect the environment in an effort to prevent as many attacks as is possible. I see this as being accomplished by first breaking up the entirety of your customer's environments into logical layers to create a defense-in-depth strategy (that is, putting up many different types of defenses so that, should one defense fail, the one after it likely will not). The goal is to have each layer in your security strategy block some percentage of attacks, so that the likelihood that an attack is successful is literally a percent of a percent of a percent.

Take the following example of a layered security strategy I often use when discussing the topic. While not perfect, it will give you an idea of how to begin thinking about the *withstanding* aspect of your cyber resilience service offering:



Let me quickly go through each of these layers:

- Perimeter – Your customer's logical perimeter now extends to the remote worker at home. Additionally, I tend to think of inbound email and outbound web requests as cross the perimeter. Each of these points of the logical perimeter need to be able to withstand an attack. Think about including a firewall, VPN, DNS scanning, and web scanning as part of your offering.

- User – The user plays a key role in phishing attacks, enabling them by their actions. Honing the vigilance of users should be a part of the *withstand* strategy. Security Awareness Training is the answer here.

- Endpoint – Look beyond simple AV and focus on Endpoint Protection solutions that provide security based on behavior.

- Identity – For the MSP that doesn't want to become an MSSP, I'd say focus here on multi-factor authentication at a minimum. Identity and Access Management (IAM) solutions can also be of value to centralize hybrid identity, but may be overkill for smaller customers.

- Privilege – Adopting the principles of least privilege principles and/or zero trust are a great idea. Practically speaking, consider separating "regular" and privileged user accounts, and use Privileged Account Management solutions to isolate the use of such accounts to those allowed to do so.

- Applications – For those applications where actions taken can have a massive impact (e.g., an Accounts Payable system, where modifying banking details as part of a BEC scam could cost your customer thousands), activity within should be monitored by

either logging or a User Behavior Analytics solution.

- Data – Access to and use of data should be monitored and audited regularly. This can be daily via a SIEM solution, and periodic use of some form of auditing solution.

Recover

I love that *recover* is included; you need to approach cyber resilience from a more holistic standpoint – one that both protects the technology that makes up your customer's operations (read: *withstand*) and the data that resides on it. Which brings us to *recover*.

Typically, when we're talking about any kind of cyber security-related services, we tend to silo out data protection as a separate offering. But, in today's world where the greatest "disaster" is a cyberattack, there's initially some distinct inherent cross over between security solutions and backup/DR solutions:

- Backup ➞ Security – When threat actors modify the environment (e.g., create user accounts, modify the membership of Domain Admins, or assign new permissions to a resource), you need to specifically recover the security configuration to put the environment back into a known-secure state.

- Security ➞ Backup – Many ransomware variants are coded to first go after something like 50 different backup file types to delete them (to make recovery more difficult). Having proper security around those backups to prevent access is key.

The practical outcome here is your cyber resilience strategy must be bookended with backups on one end and recovery on the other. I'd also add you should ideally be choosing a backup solution that will serve as the basis for Disaster Recovery and

even push you into the Disaster Recovery-as-a-Service (DRaaS) business.

There's an entire separate eBook worth of content I could go over just to properly cover proper DR, but, for the sake of brevity, I'll cover the highlights to get you working down the path towards the data protection side of cyber resilience.

1) Start with Recovery – Determine how you will recover a customer environment (e.g., on-site, in the cloud) and what the customer's recovery needs are (e.g., how quickly will you need to recover – it determines whether you're going to go the backup/restore route or continually replicate VMs). Do this same exercise for various cyberattack scenarios (data breach, ransomware, etc.). The result will be the proper selection of backup technology and methodology that will allow you to quickly recover some or all of an affected environment.

2) Prioritize – If you were solely focused on DR as your business, you'd be first performing a Business Impact Analysis where you identify the business functions, workloads, data, etc. that are critical to operations. Next comes a Risk Assessment, where you measure the impact a loss would have on operations and prioritize the severity of specific disruptions (read: each type of cyberattack you want to recover from). The result from this exercise is you having a priority of which workloads need to be protected for a given customer are most important.

3) Plan and Test – Recovery is MUCH more than just running a restore of a backup job; you should be thinking is terms of customer operations, application dependencies, OS and application compatibility, recovery order, perhaps even automated recovery orchestration. Develop some level of

recovery plan that outlines the steps needed to recover and failover (if necessary) an impacted customer (and don't forget failback!).

Then perform recovery simulations periodically to test the plan. And I don't mean tabletop walkthroughs; I mean perform an actual recovery (probably to an alternate environment) to make sure you *can* recover.

According to Forrester's *State of Business Continuity Preparedness 2021* report, 47% of organizations never perform a recovery simulation and most only do a tabletop walk though once a year!

Offering Cyber Resilience

It's obvious today's businesses – regardless of how small they are – are expected to be resilient in the face of any disruption, including a cyberattack. So, by bringing security services together with data protection services you find your business being able to offer cyber resilience services.

By thinking about the outcome first – your ability to continually protect your customers from attack and respond to a successful cyber threat and to return the customer to a working state quickly – and working backwards to the technology needed, you should be able to easily establish the practical set of solutions and services scopes needed to create a standard offering for your customers.

The SMB isn't exempt from cyberattacks. And, should one hit, they will feel the impact far more than a larger business, creating an opportunity for the MSP. In this eBook, learn about what cyber resilience means and how to translate that into an impactful, effective, and profitable service to offer your customers.

About Nick Cavalancia

Nick Cavalancia is a Microsoft MVP, a Technical Evangelist by trade, and is a 25+ year IT veteran and former MSP owner who regularly speaks and writes for some of today's most recognizable companies.