CARBONITE an opentext company | WEBROOT an opentext company

Lockdown lessons

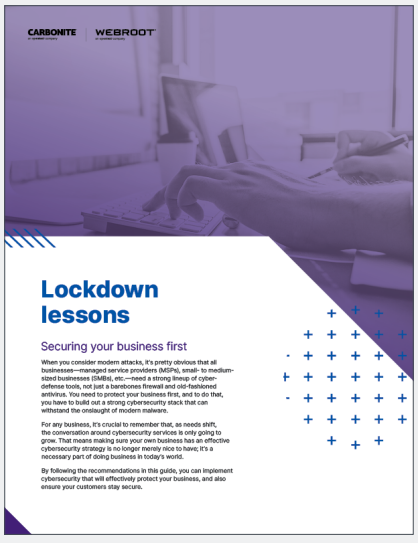
Introduction

When you consider modern attacks, it's pretty obvious that all businesses — managed service providers (MSPs), small and medium-sized businesses (SMBs), etc. — need a strong lineup of cyber-defense tools, not just a barebones firewall and old-fashioned antivirus.

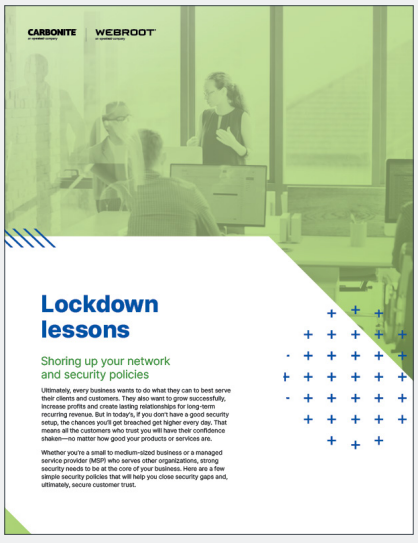
Ultimately, every business wants to do what they can to best serve their clients and customers. They also want to grow successfully, increase profits and create lasting relationships for long-term recurring revenue. But in today's cyber-climate, if you don't have a good security setup, the chances you'll get breached get higher every day. That means all the customers who trust you will have their confidence shaken — no matter how good your products or services are.

Whether you're a business or an MSP, you can use these simple tips and guidelines to implement cybersecurity strategies that will effectively protect your business and also ensure that your customers stay secure.

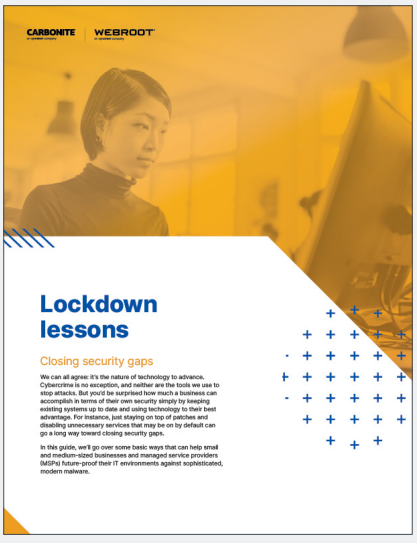
> You need to protect your business first, and to do that, you have to build out a strong cybersecurity stack that can actually withstand the onslaught of modern malware.
>
> **George Anderson**
> **Product marketing director, Webroot**



Securing your business first



Shoring up your network and security policies



Closing security gaps

CARBONITE
an opentext company

WEBROOT
an opentext company

Lockdown lessons

Securing your business first

These days, making sure your own business has an effective cybersecurity strategy is no longer merely nice to have; it's a necessary part of doing business. Follow the recommendations in this section to start building a strong cybersecurity foundation.

Did you know ... DNS-layer security can stop up to 88% of threats before they even hit your endpoint devices?[1]

Embrace automated threat detection and response

While the term "antivirus" has been around long enough that it gets the point across to just about anyone you talk to, it truly belongs in the consumer space. When you get to the business level, even if you're still talking in terms of a small office with 10 or fewer employees, you need more. You need a solution that stops threats effectively and remediates systems automatically so you don't have to spend time and resources (that you may or may not have) on manual virus cleanup.

You need a solution that doesn't just work to stop threats but actually puts time back in your day.

Enter automated threat detection and response. Look for solutions that not only mention artificial intelligence (AI) and machine learning (ML), but also how they use them to automate tasks, positively impact ROI and increase speed and efficacy. With the right technology backing its threat intelligence, a cybersecurity solution stops threats while predicting and preventing them proactively.

1 in 5 businesses lost over $1 million per DNS attack.[2]

With numbers this high, you don't even need to do the math to see how preventing DNS attacks could make all the difference to a business's success (not to mention survival). You should strongly consider investing in additional protection at the DNS layer.

Educate and train your end users

The best security in the world can't protect a business if your employees unwittingly open the door to cybercriminals by clicking a phishing link. You need to educate and empower your end users to become a strong first line of defense for your organization.

The keys to achieving results with security awareness training are consistency and pace. Annual and even semi-annual training are unlikely to give you the results you want because phishers change their techniques and hooks from month to month. The training needs to keep up with those changes and incorporate them into simulated phishing attacks and training courses. But the results speak for themselves.

After 12 months of training, end users are 70% less likely to fall for a phishing attempt.[3]

Add security at the network layer

A recent report on global DNS threats found that businesses experienced an average of nine or more DNS-based attacks in the past year, which is a 34% increase over the previous year's data.[2] As a result, the report reveals:

- 63% of organizations suffered application downtime
- 45% had their websites compromised
- Just over a quarter (27%) experienced business downtime as a direct consequence
- 26% of businesses lost brand equity due to DNS attacks
- The costs associated with a DNS attack went up 49%

Back up your data

If your end users are the first line of defense, backup and disaster recovery are your last. In the event that a threat gets through and wreaks havoc on your networks and endpoints (for example, ransomware successfully encrypts all your client records), you need to be able to restore everything from secure backups quickly and easily so you can keep business downtime to the absolute minimum.

In the event of a ransomware disaster, this setup will give you the ability to mitigate any takeover of your data and almost immediately regain the full functionality of your critical IT systems. Be sure to test your backups regularly, both for security and viability, and to develop a strong disaster recovery plan so that everyone in the organization knows their role to help get systems back up and running.

When you put all of these together, they give you a strong security foundation. Not only will it keep your business safe, but it can also help MSPs develop a more rounded offering.

To see the next-gen, predictive Webroot approach to automated endpoint threat detection and response, DNS-layer security and security awareness training, visit www.webroot.com.

To see how Carbonite backup and disaster recovery can help you gain peace of mind with complete protection from data loss, visit www.carbonite.com.

Some types of ransomware and other threats can locate and encrypt files on mapped, unmapped, external and even cloud drives. You should back up your data in at least three different places:

- Your main storage area (file server)
- Local disk backup
- Mirrors in a cloud business continuity setup

[1] Based on threats identified by Webroot after scanning real-world network traffic
[2] IDC. "IDC 2019 Global DNS Threat Report." (June 2019)
[3] Webroot. "2019 Webroot Threat Report." (February 2019)

CARBONITE
an opentext company

WEBROOT
an opentext company

Lockdown lessons

Shoring up your network and security policies

Whether you're an SMB or an MSP who serves other organizations, strong security needs to be at the core of your business. Here are a few simple security policies that can help you protect both your business and your customers' trust.

Enforce strict password policies

Password reuse is pretty common, but it's a major security risk. For example, if a cybercriminal happens to obtain an end user's Amazon.com password in a phishing attack, they may attempt to use that password to access the user's other accounts. Now, what if the end user — let's call him John — also used that same password for one of the corporate systems he accesses regularly for work? In this case, the cybercriminal could gain access to John's employer's network.

It's important for system administrators to make sure that proper rules are in place to help keep the business secure; that's where password policies come in. Password policies are a set of requirements that ensure users create strong passwords, change them regularly and store and utilize them properly.

Enforce the access policies based on "least privilege"

Regardless of your business, there's always churn. You have to onboard and offboard regularly, and employees may make lateral moves or get promoted within the company. Each time this happens, the level of access necessary for these individuals may change.

The principle of least privilege refers to the notion that employees should only have enough access privileges to perform the required job.

In terms of IT, least privilege reduces the risk that an attacker could compromise a low-level user account, device or application and gain access to critical systems or sensitive data.

You should regularly review employee access controls, permissions and privileges, giving special attention to mission-critical data, applications and sensitive network locations. You're likely to find that a lot of folks who once needed access to certain systems, files or data repositories no longer do. Leaving these systems accessible to people who don't need them to do their jobs (or, even worse, who have already left the company) is a massive security threat.

Pro tips:

- Make sure passwords are complex, using special characters, numbers, caps, etc.
- Set an expiration schedule so users have to change them regularly.
- Create a rule so users can't set the same password more than once.
- Add restrictions to lock an account after a certain number of failed login attempts.
- Enable two-factor authentication where applicable.

Segment your network

Along the same lines as enforcing the least privilege principle, segmenting your networks is a step that limits the type of network access that certain users, groups or devices may have. By dividing the network into multiple smaller subnetworks, you can ensure that sensitive information is not shared freely. This also helps restrict the amount of damage malware can do if an attack successfully infiltrates a part of the network. Ransomware and other types of malware are often designed to spread quickly so they can do as much damage as possible.

There are a variety of non-security-related benefits to this step, as well. For example, these measures can boost network performance by limiting certain traffic to only the parts of the network that need to see it. You can also use network segmentation to detect and locate technical network issues more quickly. Some admins may choose to set up "choke points" to funnel traffic that needs to be inspected, filtered or otherwise controlled. And if your business is subject to certain compliance regulations, network segmentation can help you meet them (e.g., PCI DSS requires that payment systems be separate from the rest of the network).

Network segmentation can help protect you from ransomware even if it gets through your initial defenses.

Here are a few network segmentation tips:

- Keep corporate resources separate from "bring your own device" (BYOD).
- Force new or unknown devices to use a guest network.
- Ensure guest and Wi-Fi networks can't access sensitive resources or data.

CARBONITE
an opentext company

WEBROOT
an opentext company

Lockdown lessons

Closing security gaps

You might be surprised how much a business can accomplish in terms of security simply by keeping existing systems up to date and using technology to their best advantage. Just staying on top of patches and disabling unnecessary services that may be on by default can go a long way toward closing security gaps. Follow these tips to help future-proof your environment against sophisticated, modern malware.

Patch and keep systems up to date

Unpatched software, operating systems and firmware are common vulnerabilities. For example, you only have to look at some of the major ransomware attacks that have made headlines. By exploiting security gaps in older operating systems, like when the WannaCry ransomware attack took advantage of the EternalBlue exploit in 2017, ransomware can spread like wildfire.

Malware can easily be distributed via exploit kits, which target the software vulnerabilities of older Windows® operating systems, Adobe® Flash® Player, Oracle® Java, Microsoft® Internet Explorer, Microsoft® Silverlight and other vulnerable applications.

If this happens, an exploit kit landing page can execute arbitrary code and initiate a silent drive-by download. It is critical for system administrators to keep this type of software up to date, as most infections dropped by exploit kits are zero-day threats, meaning they are totally unique samples that make it very hard for antivirus solutions to identify and block them before they can execute.

Restrict remote desktop protocol access

Cybercriminals are constantly on the lookout for systems with commonly used remote desktop protocol (RDP) ports. They then attack these ports using brute-force tactics, hoping to break through weak usernames and passwords and access systems.

Once criminals gain access, they can disable protection, deploy ransomware, create fraudulent user accounts and much more.

The following steps can help you secure RDP and prevent this type of attack:

- Restrict RDP to a whitelisted IP or IP range
- Require two-factor authentication, such as smart cards
- Use protection software to prevent RDP brute-force attacks
- Change the default RDP port from 3389 to another unused port
- Block RDP entirely (port 3389) via firewall
- Create a GPO to enforce strong password requirements
- Monitor possible intrusions using the Windows® Event Viewer (filter event logs by Event ID 4625, “an account failed to log on”)

Because many malware variants can be delivered through email attachments — typically a zip archive that contains a script — you can help prevent attacks simply by disabling scripts, including WSF, VBS, WSH, HTA and JS files.

Block known malware extensions and disable scripts and macros

One of the simpler ways to use your own operating system to help prevent malware is to block certain file extensions that ransomware and other types of malware are known to use. You can run the file server resource manager (FSRM) to help classify files and block known malicious extensions.

As a further security measure, we recommend you consider disabling macros. While Microsoft® Office macros may have legitimate uses in your specific environment, they are typically not necessary and can present a significant security risk, since some ransomware types use macros in documents as a method to deliver malicious payloads.

Invest in intelligent technology

If you've been paying attention to cybersecurity in the last past years, you know that AI and ML aren't just buzzwords, they're highly necessary for stopping zero-day threats. While these technologies may not fall into the category of using what you already have at hand as the previous tips did, they do go a long way toward future-proofing your protection strategy.

With AI and ML, you can stop threats faster and with fewer false positives, and also improve productivity and business efficiency.

By implementing intelligent security that uses AI and ML-powered detection, you can stop threats proactively through advanced behavioral analysis and contextual data. You can shorten the time it takes to detect and remediate threats, thereby reducing the cost and impact associated with an attack. Finally, you can effectively augment your workforce by using these technologies to automate basic tasks so employees are free to focus on other revenue-generating activities.

Below are two methods you can use to block scripts:

- **Redirect script file extensions via GPO**
  This method lets you set the default program to open scripts. We recommend you redirect the following file types: .hta, .jse, .js, .vbs, .vbe, .wsf, .wsh and .ps1.

- **Disable Microsoft® Windows® Script Host (WSH)**
  The Wscript host is a Windows application that interprets and executes .vbs, .vbe, .js, .jse, .wsf and other types of script files. Depending on your IT needs, you may choose to disable it entirely.

Key takeaways

- If your only security is antivirus and a basic firewall, it's not enough.
- You can stop up to 88% of malware at the DNS layer, before it hits endpoint devices.
- There's no such thing as too much end user security awareness training.
- Back up everything, in multiple places, and test backups frequently.
- Strong password and access policies are crucial.
- Segmenting your network can help prevent the spread of cyberattacks.
- Out-of-date software and operating systems could be your downfall.
- If you don't need RDP, macros or scripts, disable them.
- To future-proof your organization, you need intelligent, ML-based security.

When you put all these tools and tips together, they give you a strong security foundation. They'll keep your business safe and also help MSPs develop a better-rounded offering for their customers.

Next steps

To see the next-gen, predictive Webroot approach to automated endpoint threat detection and response, DNS-layer security and security awareness training, visit www.webroot.com.

To see how Carbonite backup and disaster recovery can help you gain peace of mind with complete protection from data loss, visit www.carbonite.com.

For more security tips, podcasts and other resources, visit www.webroot.com/LockdownLessons.

Contact us to learn more — Webroot US

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

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.