HOW TO PROTECT YOUR NETWORK AGAINST CYBERSECURITY THREATS

BY D. NOUR DANDAN | NETWORK BOX USA, LLC.

CONTENTS

05

MOVING TO THE CLOUD

06

OUTSOURCING CYBERSECURITY MANAGEMENT

07

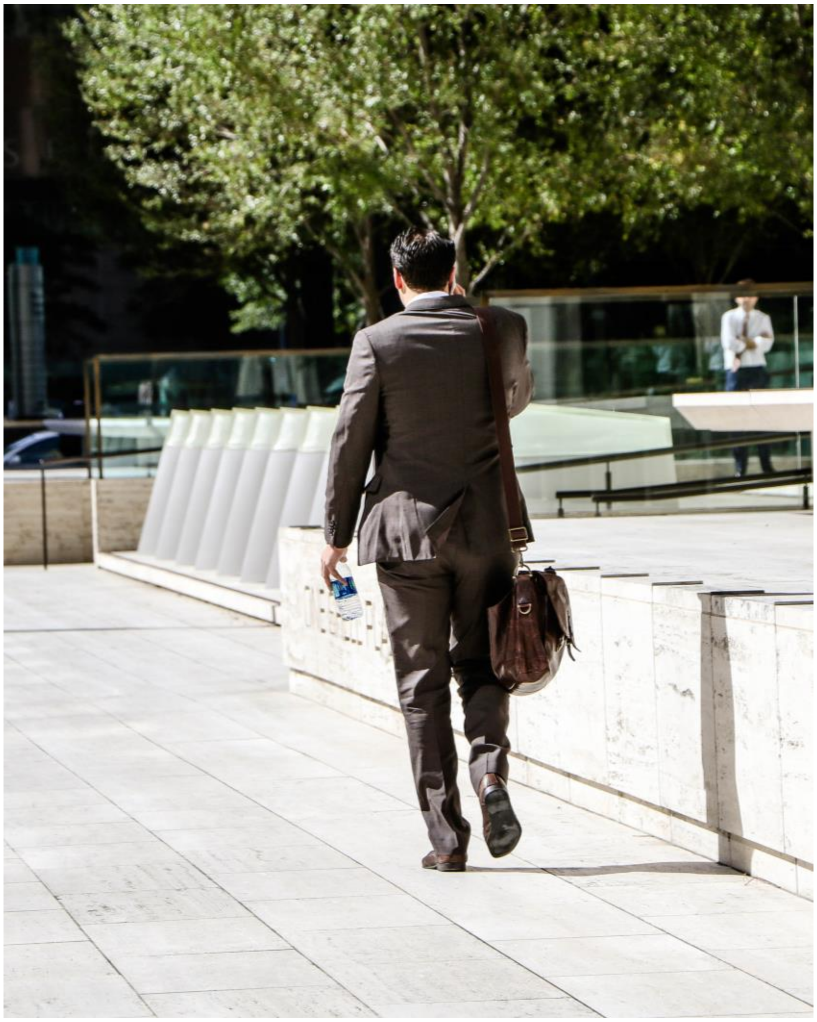
24X7 MONITORING

WHY ARE WE MORE WILLING TO UPGRADE OUR PHONES EVERY OTHER YEAR (OR EVERY YEAR), BUT NOT OUR CYBERSECURITY?

Every year since 2007, Apple has released a new iPhone model (and iOS upgrade) that leverages faster and, at times, newer technology. Most users upgrade their phones every other year, some do so annually, and the rest hold onto the older models for as long as their patience allows.

Hardware is the vessel of information technology, but it can also be its biggest obstacle. This is especially true in the cybersecurity space, which operates in a dynamic landscape. **In 2018 alone, there were over 135 million new pieces of malware.**[1] That's 135 million+ new pieces of malware that networks needed to protect against.

At that rate of threat generation, how can we expect yesterday's hardware to protect our networks today and tomorrow? Why are we more willing to upgrade our phones every other year (or every year), but not our cybersecurity?



[1] https://www.av-test.org/en/statistics/malware/

THE ROADBLOCKS

It’s relatively easy to get stuck in a cycle of technology obsolescence. This is in part due to **risk (i.e. downtime and impact) and budgets**. Upgrading your phone is a low risk transaction with little downtime that impacts an individual, while upgrading a cybersecurity solution has the potential risk of a lengthier downtime that may interrupt business operations and impact a company and its clientele. After all, cybersecurity configurations and network compatibility are more process-intensive than restoring a new iPhone from a recent backup.

IT budgets are also limited and often prevent network refreshes from moving forward. One issue is that the cost of cybersecurity involves more than just hardware. Between hiring, training, and retaining personnel to general upkeep and maintenance, the cost adds up. Furthermore, **trying to quantify the ROI (Return on Investment) of cybersecurity is an issue in and of itself.**

Risk and budget considered, there are security features and strategies companies can employ to circumvent the hardware game. These are not mutually exclusive, and each can play a key role in strengthening your security posture against future threats.

CYBERSECURITY IS

NOT JUST A SOLUTION …

… IT'S A STRATEGY.

REAL-TIME THREAT PROTECTION

When boiled down to its bare bones, **the most important aspect of any cybersecurity solution** is how and when updates (including signatures and patches) are delivered and installed. Without updates, a cybersecurity solution is truly static and more than likely outdated as soon as (if not before) it's installed.

THE HOW

Updates are delivered in one of two ways: pull or push. In the pull method, a client polls the vendor for updates; with the push method, the updates are pushed out from the vendor to the client. In other words, **pull is client-initiated, and push is vendor-initiated.**

While both accomplish the same task, push is the more efficient of the two. In a pull situation, there is the possibility that a client polls the vendor and the vendor doesn't have an update. With push, the interaction is only initiated when an update is available. Vendors like Network Box USA take the push method a step further by installing those updates once they've been delivered. The entire process is fully automated and hands-off from the client-side.

THE WHEN

When updates are delivered is equally as important as how they're delivered. The rate of threats in 2018 was approximately 4.3 new pieces of malware per second. With new threats nipping at our heels, real-time updates are critical to every cybersecurity solution. Simply, your cybersecurity solution should be **updated in less than 60 seconds upon availability of the protection** (e.g. signature, patch, etc.).

When looking at cybersecurity solutions, find one that includes automatic, real-time push updates. In today's threat landscape, anything less can easily put your network, your business, and your clients at risk.

MOVING TO THE CLOUD

Looking at the history and evolution of data exchange, virtualization and the cloud were inevitable. From mainframes to geographically dispersed data centers, every decade since the 1950s introduced another step towards where we are now – the age of cloud computing.

There are **two models**, or deployment options, when it comes to the cloud: **private and public**. In the private cloud model, a company moves its data center off-premise. In the public cloud model, a company's data and/or applications are hosted in a shared virtual environment. Some companies may opt for a hybrid deployment option, where they (for instance), host a process-intensive application in a public cloud setting, while storing sensitive data in their private cloud.

The most enticing part of moving to the cloud is its scalability. Whether a business is growing or downsizing, there is an inevitable shift in technological needs and the hardware involved, which can also impact cybersecurity. For example, if a company of 10 grows to a company of 50, their Internet traffic and web browsing activity is bound to increase. A web proxy that's configured to handle web browsing for 10 users may not be able to keep up with the significant increase in web browsing activity from the company's growth. In this case, a virtual cybersecurity solution would offer the flexibility needed to accommodate the increase in users.

All in all, the cloud is a viable option when it comes to a network refresh. In addition to the **guaranteed uptime and cost savings**, it's easily scalable and gives companies added flexibility when growing or downsizing.

OUTSOURCING CYBERSECURITY MANAGEMENT

Cybersecurity is a specialized branch of IT. Trained network security engineers must understand the ins and outs of networking, in addition to implementing and keeping up with security best practices. Between the hiring process, training, and continuing education, outsourcing cybersecurity management to a managed security services provider (MSSP) becomes a plausible option.

CHANGE MANAGEMENT

Your network is vulnerable from the moment it's brought online, and network configurations are far from a one-size fits all process. To ensure that your defenses are ready, it's critical that your network is expertly configured and that any changes/adjustments to your network are made with **cybersecurity front of mind**.

Oftentimes, when an IT admin is configuring or making a change to a network, their primary focus is on making sure everything works, which is important in its own right. However, this becomes an issue when a change leaves a network vulnerable.

Outsourcing cybersecurity management separates the roles of the individual requesting the change and the individual making the change. The network security engineer, the individual making the change, is focused on cybersecurity first; fulfilling the request becomes secondary. While this may seem like a roadblock, it's more of an assurance and an added layer that strengthens your security posture. If an IT admin places a change request that may leave their network vulnerable, the network security engineer can make recommendations on how to safely approach that change before implementing it.

YOUR NETWORK IS
VULNERABLE
FROM THE MOMENT
IT'S BROUGHT ONLINE ...

24X7 MONITORING

Outsourcing cybersecurity management can prove invaluable when it comes to monitoring your network. We constantly hear that **the Internet never sleeps, and, in turn, cybercrime never sleeps**. It's true. Regardless if it's a weekday or weekend, holiday or not, there is always the potential threat of an attack.

To maintain around-the-clock monitoring in-house, a company would need to hire a minimum of 3 full-time network security engineers. Along with salaries, a company would incur the costs associated with training and continuing education. After all, network security engineers need to stay on top of the latest threats and methodologies that hackers use. By outsourcing cybersecurity management, the cost of hiring, training, and continuing education of network security engineers becomes the MSSP's responsibility.

In-house monitoring also has its limitations; in-house network security engineers' view of the cyber land-scape is usually confined to their own network. This presents a problem in that **not all cyberattacks are targeted**. Oftentimes, we find that hackers will send something out into the wild in hopes that it sticks. How can a company protect itself from a vulnerability it didn't even see coming?

MSSPs are often backed by a Security Response Center (SRC) that, in addition to creating threat protection, monitors clients' networks globally. They have a global view of threats impacting other networks and can create all the protection necessary.

The threat landscape may be ever-changing and static solutions are, oftentimes, outdated before they're installed. Even so, there are steps you can take to leverage resources and create cybersecurity strategies that are both flexible and up-to-date. After all, **cybersecurity is not just a solution; it's a strategy.**

HOW TO PROTECT YOUR NETWORK AGAINST

CYBERSECURITY THREATS

FACEBOOK	/NetworkBoxUSA
TWITTER	/NetworkBoxUSA
LINKEDIN	/NetworkBoxUSA
YOUTUBE	/NetworkBoxUSA
INSTAGRAM	/NetworkBoxUSA
BLOG	networkboxusa.com/blog
WEBSITE	networkboxusa.com

NETWORK BOX USA
cybersecurity done right

2825 Wilcrest Drive
Suite 259
Houston, TX 77042

832.242.5757

info@networkboxusa.com