


Learning from COVID-19: Security and Continuity Planning

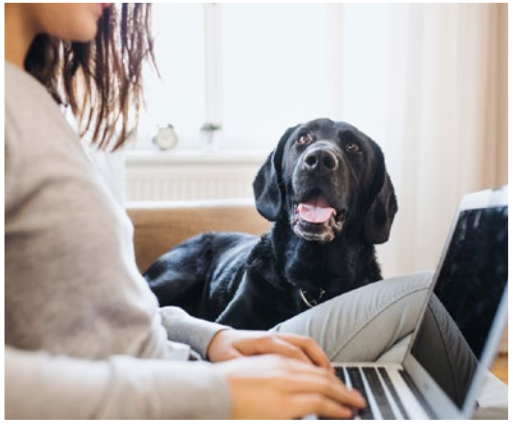
WatchGuard®

Table of Contents

INTRODUCTION

As society confronts a major pandemic, Novel Coronavirus (COVID-19) is impacting nearly all people around the world. Schools are closed, travel is restricted, events cancelled, and offices emptied – all with the goal of stemming the spread of COVID-19. The Center for Disease Control has even suggested employers establish polices that allow their employees to work remotely to promote social distancing. Heeding the call, businesses have rapidly mobilized to meet the threat, and as a result, more people today are working from their homes than at any time in modern history. And just to give you an idea of how disruptive that may be, according to a study, the remote workforce in America grew 159% between 2005-2017. It's safe to say that today, due to the coronavirus outbreak, we are looking at vastly higher numbers.

While the response to coronavirus has been unprecedented, for many businesses this "work-from-home" experiment launches them into decidedly unfamiliar territory. In this eBook we will outline the strategies for maintaining business continuity during the coronavirus outbreak.



COVID-19 LANDSCAPE ANALYSIS:
CURRENT CHALLENGES TO BUSINESS CONTINUITY

We face risks in cybersecurity every day. However, one of the challenges of enabling a mobile workforce is that the chances of being the subject of cyber attacks can increase significantly. Without the benefit of your core network protections, a user on the go could become infected without your knowledge, and even introduce the infection to your broader environment when they reconnect with your network.

Hackers exploit coronavirus fears

It seems hackers will take advantage of any major news story or world event to launch their attacks. At a time of heightened fear, your employees' email and social media accounts are flooded with news reports, comments, videos, and links about the virus. Unfortunately, cyber criminals are exploiting fears to phish your users, hack their systems, or deliver malware.

Here are just a few examples of how threat actors are taking advantage of coronavirus:

- **Impersonating the World Health Organization** (WHO). The WHO reported suspicious phishing messages that impersonated their organization and purported to give critical health information. Victims were asked to click a link, download a file, or provide sensitive information.
- **Delivering Malware.** A group of hackers has leveraged the coronavirus pandemic to infect victims in Mongolia with a previously unknown malware, in a recently discovered campaign that's called "Vicious Panda."
- **Spamming the Emotet Trojan**. Hackers use seemingly helpful notices about how to prevent the spread of coronavirus targeted users in Japan as part of a spam campaign designed to introduce the Emotet trojan. Emotet is capable of hijacking email accounts and spoofing messages to further infiltrate an environment.
- **Fake Virus Tracking App Delivers Ransomware.** An app masking itself as a coronavirus outbreak map tracker is actually ransomware that locks down your phone. The app, "COVID19 Tracker," infects your device and demands $100 in Bitcoin within 48 hours.

Off-Network Newbies

COVID-19 is driving aggressive work-from-home policies, with businesses shuttering offices and sending the bulk of their employees to work from home full time almost overnight. While workplace flexibility is now the norm for many businesses, the average company sees around only 30% of their workforce working from home at a given time. Many companies have struggled to provide the resources needed to keep folks secure when working from home, issuing hastily provisioned laptops, or sending them home with desktops never intended to be taken off the secure network. Not only do these devices need security now that they are off-network, its important that we make sure they don't introduce malware and other threats when they re-connect to the network, either by VPN or returning to the office.

VPNs Are Overloaded

With coronavirus scattering employees to their homes, VPN usage has skyrocketed, with researchers noting a 50% increase in traffic in a one-week period. The United States alone is expected to increase VPN use by 150% in a month's time. The sudden migration of users from corporate to home offices has left many businesses scrambling to provide VPN licenses to their employees. The risk is that without VPN connectivity, users will not have access to the resources they need or they will use insecure connections to access them.

Bandwidth Bedlam

It's not just your employees who are home. With schools closed, many of your coworkers will have children at home continuing their education remotely, gaming, or simply surfing the web. Both parties will quickly gobble up bandwidth, especially when using resource-intense applications like video conferencing. Places hardest hit by the virus have seen over a 90% increase in Internet use. In response, many ISPs are upgrading their customers to faster, higher bandwidth offerings, or eliminating data caps to avoid overages.

EIGHT TIPS FOR IT LEADERS TO USE SECURITY AS AN ENABLER OF PRODUCTIVITY AND ACCESS

1. INVENTORY AND ASSESS YOUR COMPANY'S REMOTE WORK CAPABILITIES

While 92% of businesses offer remote work, the opportunity has not been afforded to all employees equally. For many companies, this shift to remote working happened almost overnight, leaving little time for adequate planning. Now is the time to audit and assess the new network access your company needs and consider the security implications. Managed Security Services Providers (MSSPs) are experts in security assessment, and can help midsize businesses quickly come up to speed and get their users what they need.

For network nomads, who are always on the go, chances are they have the resources they need for the long haul. For the folks who haven't worked from home as much, it is helpful to take an inventory of all of the data and applications they may access regularly. From there, you can map out what needs to be accessed, who needs access, and how best to provide that access. Work with department heads to understand the unique needs of their team and make sure their team members are set up for success.

Here is a checklist of things to consider:

- ✔ Does the employee have a sanctioned device, or do you need to acquire more phones/laptops?
- ✔ Do you have enough VPN licenses to issue to all that need them, or do you need to acquire more?
- ✔ Does the employee have sufficient Internet access to perform their job?
- ✔ What systems does the employee require to do their job?
- ✔ Does the employee require secure access to sensitive systems and data?
- ✔ What Cloud applications does the employee use on a regular basis?
- ✔ Is the employee set up to use multi-factor authentication?

2. SET AND COMMUNICATE EXPECTATIONS FOR REMOTE WORK

As many of your employees are likely working from home for the first time, now is a great time to reach out to your team to outline your company's work-from-home policy to set expectations for employees working remotely. Some 24% of businesses haven't updated their work-from-home policy in over a year, so use this as an opportunity to do so. A simple email, or conference call with your team, can go a long way.

Some things you may want to address:

- **Availability** - What hours do you expect your team to work? When are you making yourself available?
- **Responsiveness** - Are remote workers expected to respond immediately? If so, how will that expectation be communicated? For example, will truly urgent requests only be made via phone?
- **Platforms** - Remind your employees which tools and platforms they should be using, including the Cloud storage platforms, communication/video conferencing tools, project management tools, etc. Encourage your team to avoid all other non-sanctioned platforms.
- **Devices** - If your team has company-issued devices, remind them of any policies you have established around their use. If they are using their own personal devices for work, now is a good time to provide guidance on which devices are appropriate to use and how employees are to conduct business on those devices.
- **Incident Reporting** - Where should an employee go if they feel like the company's information may have been compromised? Who should they report the breach to, and what steps should they take to minimize the fallout?

3. FOSTER A CULTURE OF CYBERSECURITY

Most business leaders understand that the culture of a workplace is an important part of what drives its success or failure. They must also come to understand that the same dynamics exist in cybersecurity. As your employees are under threat from targeted attacks, in some instances impersonating members of your team, corporate culture often ends up being the difference between intercepting the attack or infecting your entire network.

Hackers use techniques to manipulate and influence your users into taking the action they want, using authority and urgency as a weapon. As a leader, you should encourage open channels of communication, so when an employee, even at the lowest levels of the organization, sees something they believe is a threat they feel empowered that their concern will be taken seriously.

Tips for fostering a culture of cybersecurity:

- **Share stories.** Employee catch a phishing email or have their laptop infected with ransomware? Sharing the story among the company can help to make the stakes real in the minds of your employees and help others avoid similar attacks. Sharing news about attacks against similar businesses can also help.
- **Reward behavior.** When an employee reports a potential attack, they could be saving your business a major headache, so why not reward their behavior? Incentivizing employees to report suspicious activity can help drive awareness and get others involved.
- **Be nice.** Let's face it, businesses are made up of people of widely varying technology skills. It's simply not realistic to think that your employees are going to avoid every threat and follow every policy. People make mistakes. That's why it's so important to be supportive.

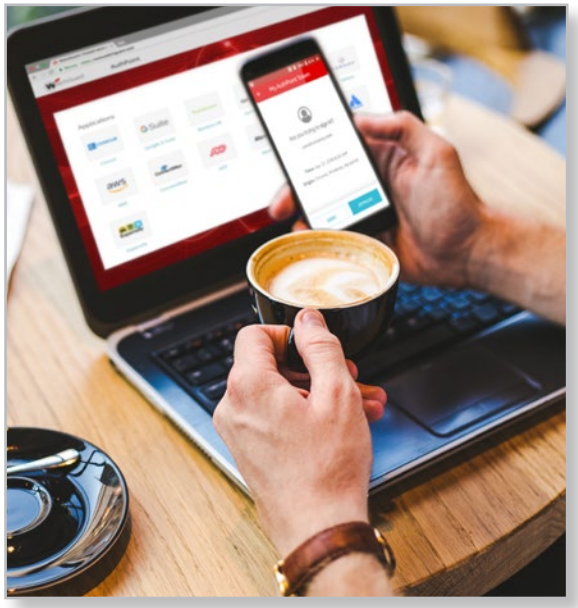
4. IMPLEMENT MULTI-FACTOR AUTHENTICATION

As companies grapple with having the predominance of their workforce working remotely, securing access to internal tools presents a major challenge. At the same time, hackers are increasingly targeting credentials, placing your users' account information directly in their crosshairs. For this reason, we recommend deploying multi-factor authentication (MFA) to all of you users, so they are fully authenticated every time they connect to your network.

Multi-factor authentication also allows you secure access to Cloud applications and environments that remote workers might access directly from the Internet, adding an additional layer of protection at a time when businesses are most vulnerable.

What to look for in an MFA solution:

- **Cloud delivered.** Unlike MFA that requires a hardware token, Cloud-based solutions make it possible for a user to download an application to their phone and get up and running immediately.
- **Application coverage.** Your solution should integrate to protect all of the critical applications your employees may need.
- **Simplicity.** The solution should be intuitive for users of varying technical ability.
- **Multiple authentication methods.** Support for multiple online and offline authentication options ensures authorized users can access what they need, when they need it.
- **Supports multiple tokens.** MFA is now commonly offered by social media sites, banks, retailers and more. Look for a solution that allows you to consolidate tokens to a simple MFA application to streamline access for your users.



5. EXTEND VPN ACCESS TO PRIORITY USERS

Secure connectivity to corporate headquarters and critical applications is essential if your employees are going to maintain productivity as they work remotely. Virtual Private Networks (VPNs) add a layer of security to private and public networks, allowing individuals and organizations to send and receive data safely over the Internet.

Generally, your users will require one of two VPN types:

1. **Client-based VPN.** Operating at the network layer, a client-based VPN provides users access to the entire network.

2. **Client-less VPN.** Typically requiring only a browser, client-less VPNs connect users to specific applications and services.

Normally businesses only provide VPNs for a limited group of remote and frequently travelling employees, as opposed to the entire staff. As VPN usage balloons, here are some tips to help you manage your usage and avoid disruption:

- **Prioritize VPN for high-risk users first**. Some employees will require greater access than others, and still others may not need VPN access at all. Understanding who needs access, to what, and making VPN available based on priority will help avoid overburdening the network.

- **Use a firewall in the Cloud to keep up with demand.** The spike in demand for VPN services doesn't mean you have to clear space in the server room. Cloud-hosted firewalls can help to load-balance VPN traffic destined for your HQ and scale to accommodate the connections your company requires.

- **Require MFA.** Without MFA a single set of VPN credentials could give an attacker full access to your network. Users connecting using a VPN should be fully authenticated using a minimum of two factors.

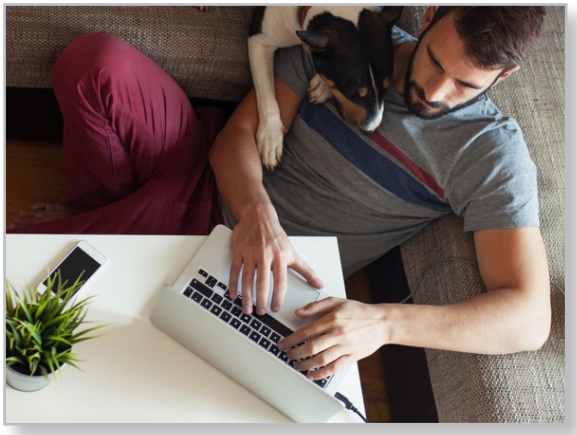
- **Issue a tabletop firewall.** A tabletop firewall deployed in a user's home office can provide full UTM protection without burdening your corporate VPN.

6. KEEP USERS SAFE FROM RISKY CLICKS WITH DNS FILTERING

Keeping users safe as they navigate the Internet is more difficult when they are connecting from outside of your network. With employees stuck at home, chances are good that company laptops will be used for a hefty amount of personal web surfing and email checking. Cloud-based DNS filtering makes it possible to block connections and limit access to the risky areas of the Internet. Clicks on malicious links or attempts to connect to domains related to phishing and malware can be prevented, without having to use a VPN.

Things to consider in a DNS-filtering solution:

- **Productivity and policy enforcement.** With more employees working off-site you may also want to restrict your users from accessing certain types of content, like social media and adult sites, for productivity reasons. Look for granular controls, like the ability to block users and groups, as well as establish hours of enforcement.
- **Support for security training initiatives.** By now most companies have some form of cybersecurity training for their employees, but as they migrate off-site, reinforcing that training is more important than ever. Some DNS-filtering solutions not only block bad connections, they provide the user a refresher on how to identify similar threats in the future.



7. KEEP ENDPOINTS FREE OF MALWARE

Malware and ransomware threats have only accelerated as a result of coronavirus. And the risk of infection has never been higher, as users may no longer benefit from the protection of a firewall when working from home. While endpoint antivirus solutions will catch many of the threats, they are powerless against evasive, zero day malware that we see all too often. Endpoint detection and response (EDR) solutions can not only detect these advanced threats, they can kill the threat and return the infected device to good order, 100% remotely.

Essential features of an EDR solution:

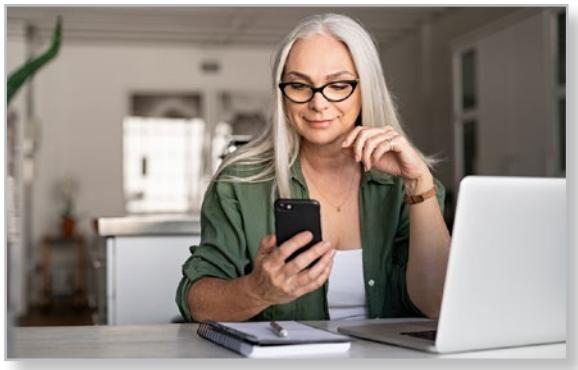
- **Detection methods.** Catching advanced malware takes advanced techniques. Look for solutions that combine several detection methods, including behavioral, heuristic, and sandbox analysis.
- **Automation and AI.** Responding to threats quickly can save a major headache. Automating detection and response can make this near instantaneous.
- **Host isolation.** When a threat is detected, the infected host should be removed from connectivity with other parts of your network to avoid spreading infection.

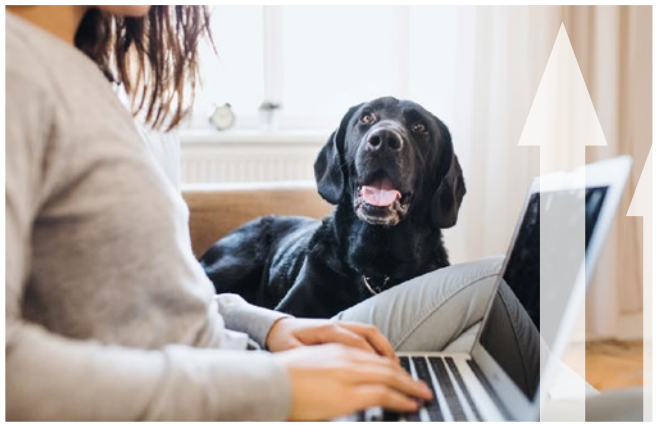
8. Retain Control of Wi-Fi

Working from home can introduce security concerns related to Wi-Fi as well. For remote workers located in dense housing areas such as apartments or condos, every Wi-Fi device including doorbells, gaming consoles, and IoT devices can be a way in for malicious neighbors looking to eavesdrop. Nefarious neighbors could exploit the fact that their building is full of folks working from home, with Wi-Fi making up nearly 50% of all IP traffic.

Wi-Fi considerations for remote work:

- **Consider issuing Trusted Wireless Environment certified access points**, like the WatchGuard AP225W, to give your IT department full visibility into client and network performance so they can better support the remote workforce.
- **Preconfigure access points** for easy deployment for users at home.





In dense housing areas such as apartments, Wi-Fi makes up nearly **50% of all IP traffic**.

WHY BUSINESS PREPAREDNESS MATTERS IN IT SECURITY

Simply put, there are things you can't predict. Business leaders know there will be bumps on the road and unplanned events along the way. So, what can you do to protect your business future? A preparedness plan does not promise perfection, but it can give you the tools to securely navigate challenges and provide necessary resources to ensure operational continuity.

Today it is the coronavirus outbreak, but it could be anything and more than just disasters. A major event like The World Cup that disrupts how a city normally functions, or even human error can push your business to go on critical preparedness mode. Any situation that forces you to adapt quickly to unexpected changes is the ultimate proof of how important it is to truly understand your organization and what needs

Why? Because it shows your employees, customers, and stakeholders that your company can thrive even during unprecedented events. Yes, it's great for your brand, but more importantly, it creates great sense of trustworthiness in your community. Plus, you'll have an incredibly valuable story for years to come.

Why? Because it shows your employees, customers, and stakeholders that your company can thrive even during unprecedented events.

IT BUSINESS CONTINUITY CHECKLIST

Assessing your company's remote work capabilities

Is My Business Prepared?	Yes	No	Action
Have you updated your work-from-home policy in the last 12 months?			
Have you communicated policy and expectations for all employees now working from home?			
Do you need to acquire more phones/laptops to ensure all employees have a sanctioned device?			
Do you have enough VPN licenses to issue them as needed?			
Does the employee have sufficient Internet access to perform their job?			
Have you identified if remote employees have access to systems or platforms required to successfully perform their job? *i.e. Cloud applications*			
Is your company able to provide secure measures to avoid cyber attack risks when working remotely? i.*e. Protected Wi-Fi; VPN Connection; Multi-Factor Authentication*			
Do you need to make adjustments to your IT budget to deliver necessary resources?			
Do you need to offer remote work security training to your staff?			

FREE SERVICES TO HELP SMALL AND MIDMARKET COMPANIES DURING THE CURRENT UNPRECEDENTED EVENTS

For a limited time, WatchGuard is offering free or discounted services to help companies secure their remote workforce. Visit our **Remote Workers Resource page** to learn about special deals on WatchGuard Passport; a bundle of user-focused security services designed to block phishing attempts, enforce web policy, and authenticate people anywhere in the world.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit **https://www.watchguard.com.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

WatchGuard

North America Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com