CORONAVIRUS
THE DAY AFTER

Abstract

Early in 2020, a global pandemic caused by the spread of the Coronavirus/COVID-19 altered the lives of people forever. Once thriving organizations were suddenly paralyzed, and they're seeking ways to recover. Although the effects will be felt for years to come, there is light at the end of this very dark tunnel.

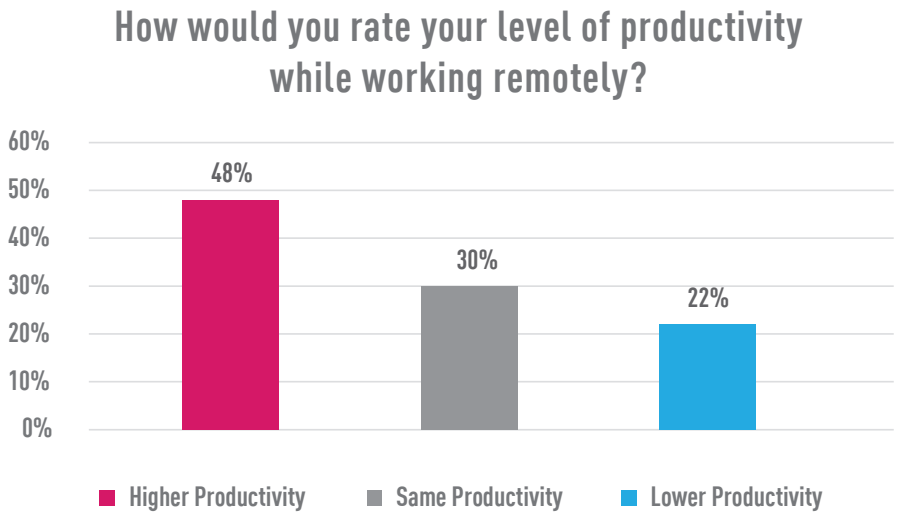
In this paper, we provide perspectives and possibilities as we move forward. We offer cybersecurity tips for you to consider as your organization reaches its new normal.

The world has changed

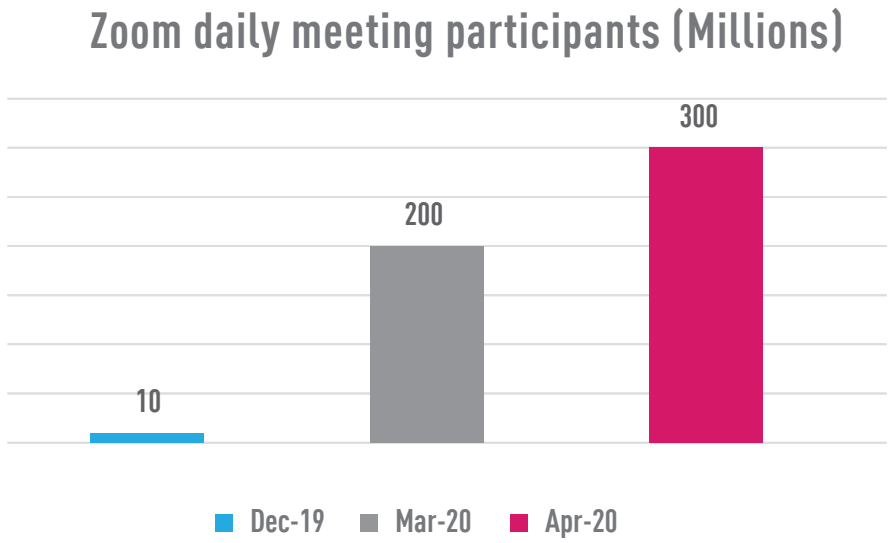
The Coronavirus/COVID-19 pandemic created a phenomenon in our entire working culture. The shifts were global, rapid and widespread, and they are entailed in the following:

1. **Remote work as the new norm**—countries mandated lockdowns (different terms describe this depending on the country e.g. shelter in place, isolation etc.) accelerated transition of employees working from home accessing corporate resources through secure access (e.g. VPN). Here at Check Point, for example. In just two weeks the **99%** of the organization moved to work from home, for the first time in our history. And this was not a rare example. When we asked our employees about this "new normal," **78%** of them reported that their productivity was the same or even higher. In a recent Gartner CFO survey, **74% of companies** said they intend to shift employees to **work from home permanently**. First company to implement this was Facebook that announced it will permanently shift 50% of its employees to remote work.

   The "new normal" is not going anywhere.



2. **Collaboration tools use is "zooming" up**—the fact that face-to-face meetings were not possible, people have been using more collaboration tools such as Zoom, Teams and Slack than ever before. Zoom, for example, had 10 million daily meeting participants in Dec. 2019 and by April 2020 they reported over 300 million—**a whopping 3000% growth!**



3. **Increased pace of Digital Transformation and move to cloud**—A recent survey by Fortune magazine showed that 75% of Fortune 500 CEOs said the crisis forces their companies to accelerate their technological transformation with cloud resources at the top. At the same time, they need to add more elements to support their business operations. This created a—"Just Do it" mindset—as a new, pressing directive for their IT Departments. And as we all know, when projects need to meet the burning demand of connectivity, the inevitable question is—have we cut some corners?

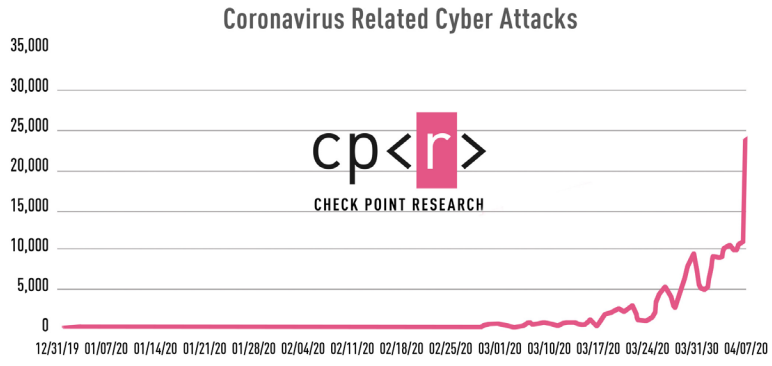
If the answer is yes, this means that your risk posture has been affected. This is not a "new normal" behavior you can afford to keep.

Culture eats security for lunch

In its insight report on COVID-19, the World Economic Forum found that out of 350 of the world's top risk professionals, **50% are worried by cyberattacks** and data fraud due to a sustained shift in working patterns.

The "new normal" changes described above produce several elements which influence the risk posture of the organization. Here are the main ones you should consider:

1. **Social-engineered attacks exploiting fear, uncertainty and doubt**—The World Economic Forum recently reported that the "demand for information on the new virus, accompanied by fear, confusion and even the boredom of confinement, has multiplied opportunities for cybercriminals to deliver malware, ransomware and phishing scams." Check Point research teams found a dramatic rise in cyberattacks in correlation with the spread of the virus, and an alarming amount of phishing attacks trying to exploit this fear. Covid-19 was not just a virus, It is a major, successful, attack theme.



2. **The attack surface grew exponentially**—With the rush to enable remote access to corporate assets, many companies allowed connectivity from **unmanaged home PCs.** Most of the time, these computers lack patches, updated best-of breed anti-malware, or any kind of protection. The only "call for duty" these PCs have is the video game carrying that name. Given the restrictions imposed almost globally, many critical services were handled by individuals which were granted remote access to **critical infrastructures'** management systems (e.g. water, trains, elevators and traffic lights). Personal mobile devices are allowed access to network more than ever before, and many apps are **moved to cloud** for scale purposes. However, many Infosec and DevOps teams rushing to the cloud didn't scale their cloud security posture to the level of their traditional data centers. This gap, in simple words, presents a dangerous opportunity for hackers.
3. **Employees are now the "CISO" of their house**—with the drastic shift to allow work from home, we face a reality where our living room is now part of the company's perimeter. Your 8-year-old is like the new employee who has access to your own network and files. In this situation, data is more in motion than ever before. Every company now needs to rely more on each and every of its employees to guard the data. If you keep your company's previous security policy with this "new normal"—you're fighting the "old war" and you're destined to be under attack.

THE PANDEMIC WILL DISAPPEAR. ITS CYBER EFFECT WILL NOT.

Stay safe. Act now.

The trends of the Coronavirus have dramatically changed the way we work, and these changes are here to stay. The accelerated pace of digital transformation, remote access infrastructure, the drastic move to the cloud—these have already gotten the attention of cybercriminals. When we change to way we work, we must adapt the way we secure our work. The "new normal" requires an updated approach of cyber security.

Here are our top tips:

Real Time Prevention

As we all know, vaccination is better than treatment. In cyber security as well, real-time prevention is the key to preventing the next attack.

Secure Your Everything

Every part in the chain matters. The "new normal" requires organizations to revisit and check the security level and relevance of their network's infrastructures, processes, compliance of connected mobile and PC devices, IoT, among others..

The increased use of the cloud means an increased level of security, especially in technologies that secure workloads, containers and serverless applications on multi- and hybrid-cloud environments.

Consolidation and Visibility

So many changes in the company's infrastructure present a unique opportunity to check your security investments. Are we getting what we really need? Are we protecting the right things? Did we miss a blind spot? The highest level of visibility, reached through consolidation, will guarantee the best effectiveness. You need a unified management and risk visibility to your entire security architecture and this can only be achieved by reducing the number of point product solutions and vendors.

Your cyber security solutions must be simple to use and easy to operate if you want to achieve the best protection. Here is a useful matrix for you to use to keep safe.

CHANGE	EFFECT	RISK	TOP PROCESS/TECHNOLOGIES TO MITIGATE (PARTIAL LIST)
Working from home	Personal mobile and computers provided access to corporate networks	Data breach (e.g. key logger, screen logger on pc/mobile)	1. Implementation of endpoint security and hygiene with compliance check (latest patches, AV...) 2. User training awareness (e.g. phishing simulation) 3. Mobile threat defense on mobile
Rapid move to cloud	Speed of deployment on the expense of security	Basic security controls can lead to data loss and manipulation	1. Invest in Cloud Security posture management 2. Deploy workload security for containers and serverless apps. 3. Real time prevention of threats with IaaS security
Critical infrastructure	Allowing critical infrastructure remote access	Critical infrastructure breach	1. IoT security for IoT devices 2. Bolster network security posture with red team... 3. OT security with Scada enforcement
Increased network capacity	More throughput is needed to address data in motion	Lack of service Network is down	1. Invest in network security that scales according to needs 2. All protections must be enabled while keeping business continuity 3. Scalable secure remote access

To summarize, as we've all learned in the past several months, in times of crisis, we need to **be agile and act swiftly**. The pandemic may be over, but the effects are here to stay, and the best way for all of us to stay connected is by being protected. The "new normal" requires us to continue to change and adapt.

To learn more about staying safe with Check Point security solutions, visit https://www.checkpoint.com/cybersecurity-the-new-normal/ for practical tips and recommendations.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2020 Check Point Software Technologies Ltd. All rights reserved.