
# CYBER SECURITY IN THE AGE OF CORONAVIRUS

# 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. It should not be forgotten that cyber security investments have and will continue to pay off for organizations. We offer cybersecurity tips for you to consider as your organization reaches its new normal.

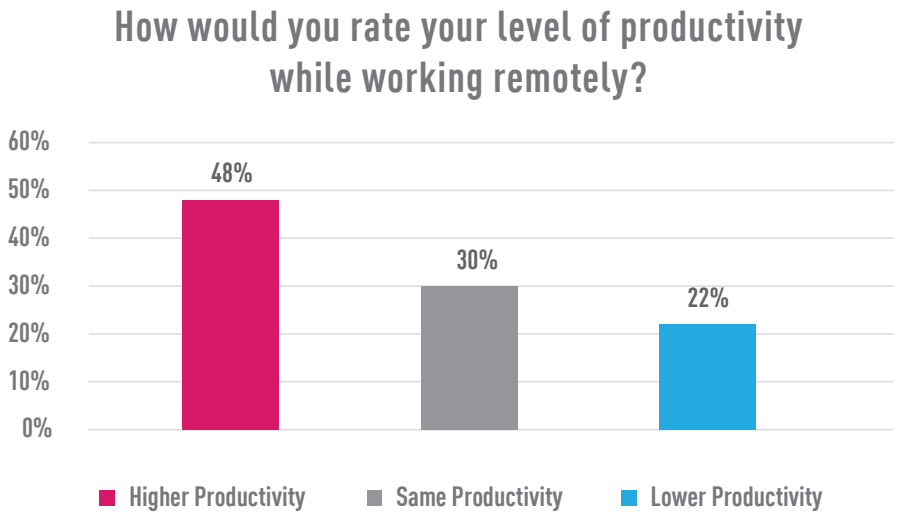

# The world has changed

The Coronavirus/COVID-19 pandemic has impacted our entire working culture. A recent survey indicates that 95% of security professionals are facing added IT security challenges due to the coronavirus. The shifts were global, rapid, and widespread, including the following:

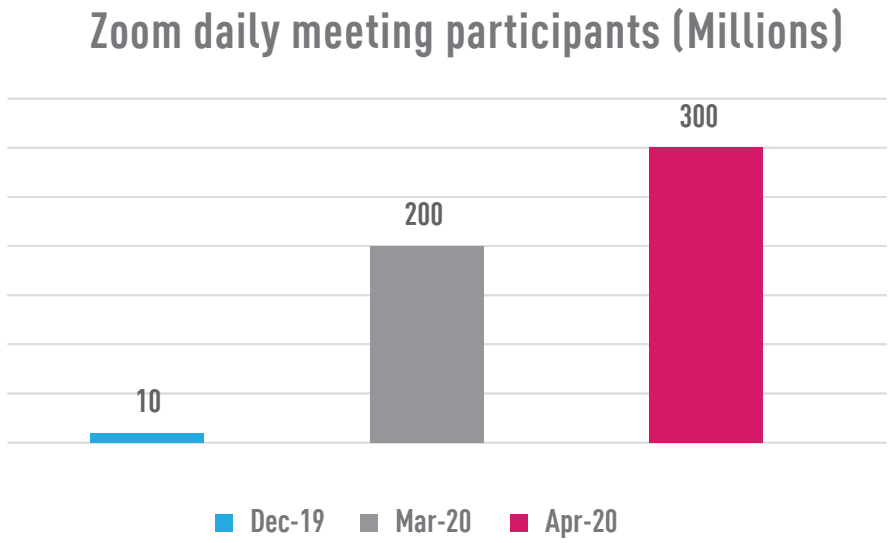
1. **Remote work as the new norm**—country-mandated lockdowns (different terms describe this depending on the country e.g. shelter in place, isolation etc.) accelerated the transition of employees to work from home, allowing them to access corporate resources through secure access (e.g. VPN). At Check Point Software, for example,in just two weeks, **99%** of the organization moved to home offices, for the first time in our history. And this was not a rare example. When asked about this "new normal," **78%** of our employees 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**. The first company to implement this was Facebook, announcing it will permanently shift 50% of its employees to remote work.

   It appears this 'new normal' is here to stay.

> " But the pandemic is more than a test: it is the accelerant for the next phase of the digital revolution. Many of the digital solutions embraced during the crisis will gather momentum in the post-COVID-19 environment."
>
> **— Lou Celi, CEO, ESI ThoughtLab**




2. **Collaboration tools use is "zooming" up**—with face-to-face meetings no longer possible, people have been using collaboration tools such as Zoom, Teams, and Slack, more 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 any corners?

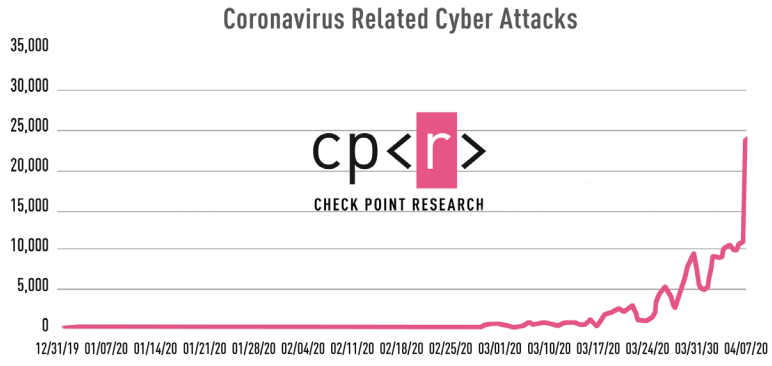
If the answer is 'yes,' then your risk posture can be affected. This is a behavior you can ill afford to keep.

# New work model heightens security risks

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 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 is 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.** Many of 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). Additionally, personal mobile devices are now often allowed access to networks, and many apps are **moved to cloud** for scalability. 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 has created a dangerous opening for hacking and cybercrime. The concerns appear justified. In May, 2020, cyber security researchers saw nearly 200,000 coronavirus-related cyberattacks per week, a 30% increase over prior weeks.

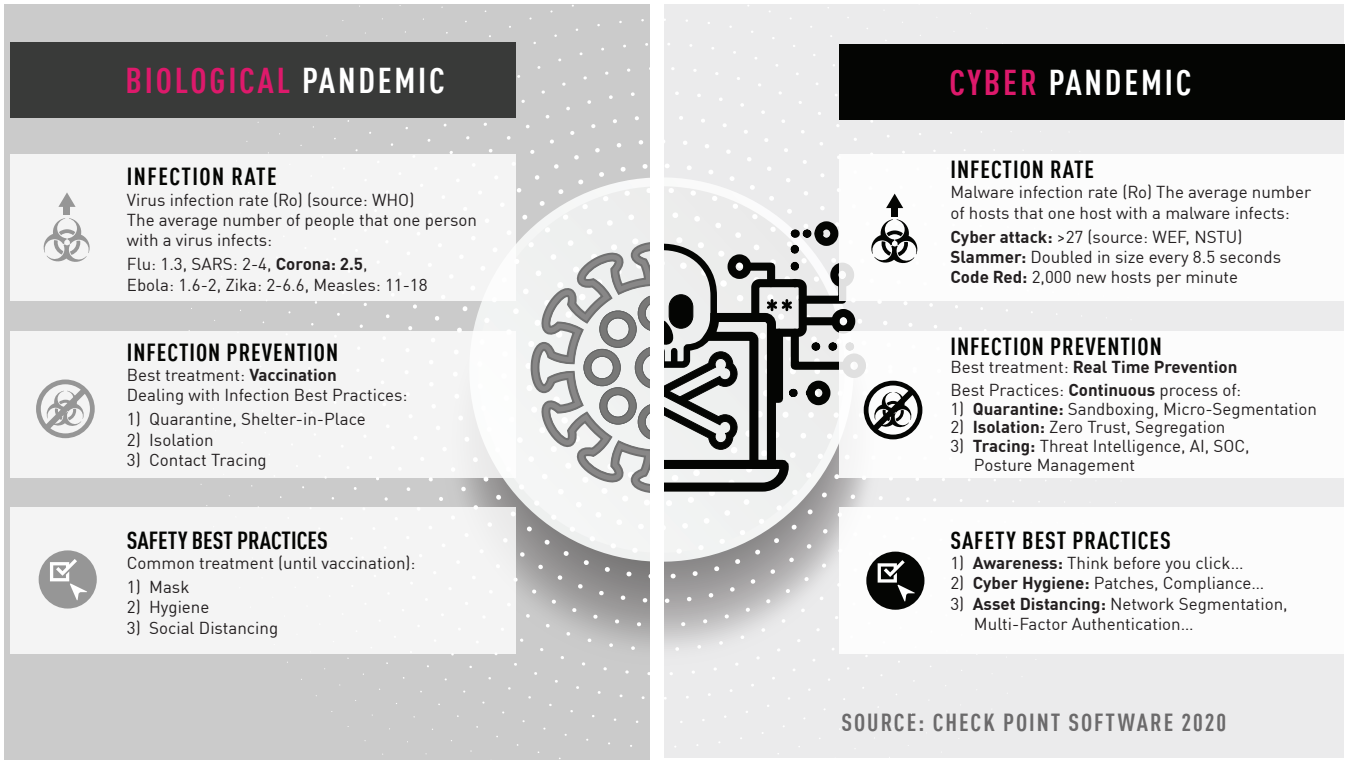
3. **Employees are now the "CISO" of their house**—With the drastic shift to work from home, our living rooms are is now part of the company's perimeter. Picture your 8-year old with access to your own network and files. In this situation, data is now more fluid. Every company must now rely more on each and every employee to guard the data. Maintaining your company's previous security policies in this new age of the coronavirus is not viable against the increasingly more potent cyber attacks.

> The most significant opportunity to arise from the pandemic is for states and individuals to realize the potential of a truly global digital society.
>
> **— "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications," WEF, May, 2020.**

# THE PANDEMIC WILL DISAPPEAR. ITS CYBER EFFECT WILL NOT.

The World Economic Forum and Zurich Insurance note, "Technology is enabling the 'contact-free economy' through applications such as telemedicine, on-line retail, and social distancing delivery methods such as click and collect. New business and employment opportunities are being created in these sectors, but a greater dependence on technology has also increased cybersecurity risks."[1]

In its analysis, the WEF warns, "We should prepare for a COVID-like global cyber pandemic that will spread faster and further than a biological virus, with an equal or greater economic impact."[2] The graphic below illustrates what Check Point Software researchers see as a parallel between the COVID-19 pandemic and the increased chances of a cyber pandemic.




[1] "Several crises in one: what effects will COVID-19 have on the global risk landscape?," by John Scott, Zurich Insurance Group, May 19, 2020

[2] "What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack," by Nicolas Davis, World Economic Forum, June 1, 2020

# 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, and the rapid move to the cloud—are known trends by cybercriminals. When we change the way we work, we must adjust how we secure our work. Cyber security strategies must be revamped to meet our new reality.

Here are our top tips:

## Real-Time Prevention

As we all know, vaccination is better than treatment. Likewise, in cyber security, real-time prevention is the key to protecting our organizations and employees from a cyber attack of cataclysmic, cyber pandemic proportions.

## Secure Your Everything

Every part in the chain matters. Organizations must 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 increase effectiveness. You need a unified management and improved 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 to keep you 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 (MFA, latest patches, AV...)<br>2. User training awareness (e.g. phishing simulation)<br>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<br>2. Deploy workload security for containers and serverless apps.<br>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<br>2. bolster network security posture with red team ...<br>3. OT security with Scada enforcement |
| Increased network capacity | More throughput is needed to address data in motion | Lack of service<br><br>Network is down | 1. Invest in network security that scales according to needs<br>2. All protections must be enabled while keeping business continuity<br>3. Scalable secure remote access leveraging micro segmentation |

"Rather than thinking of the coronavirus and stay-at-home orders as an obstacle, CISOs should see the situation as an opportunity to demonstrate our strength and capabilities. Many organizations have been able to react swiftly, change systems, and enable our enterprises to keep going. Executives have felt the importance and positive influence that the cyber security team has on day-to-day operations."

**— Jony Fischbein, CISO, Check Point Software**

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 will wind down, but its effects are here to stay, and the best way for all of us to stay connected is by being protected. Today's new reality requires us to continue to change and adapt. With cyber security now considered a business enabler, security executives will play a key role to navigate their organizations safely out the coronavirus pandemic crisis.

To learn more about staying safe with Check Point security solutions, visit https://www.checkpoint.com/cybersecurity-protect-from-cyber-pandemic/ for additional 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.