ODYSSEY™ cybersecurity

HOW THE CORONAVIRUS (COVID-19) PANDEMIC TRANSFORMED THE CYBER-THREAT LANDSCAPE

In March 2020, businesses all over the world were called to adapt, within a span of just days, to the reality of a global pandemic, and the social distancing measures that were enforced to slow it down.

This meant that companies around the world had to swiftly introduce ways to enable their workforce to work remotely thus minimizing the impact of the pandemic on their people, their clients and ultimately their financial stability and viability. In some cases, not only did organizations continue to serve their customers' interests during the outbreak without any reduction in service quality, but they even further improved their output.

When schools and universities were first shut down in March 2020, they managed to transform overnight their teaching methods and homeschooling facilities, not to mention their examination and homework assessment processes. Many retail businesses now work with online orders, payments and home deliveries, while most desk jobs have migrated to the home. Every home has now become a workstation, and high-level business meetings have moved from the hotel lobby to the realm of teleconferencing.

Tasks that were previously thought impossible to be conducted over the internet are now being completed even faster when done remotely. Teamwork and the human factor are still being maintained through innovative communication solutions that help people collaborate and work together. Rush hour traffic is a thing of the past, and environmental concerns have opened our eyes to what remote working can do to improve the quality of our lives.

Payments have shifted to more and more cashless transactions and online money transfers to avoid human-to-human proximity, not to mention transferring potential infectious disease through the exchange of physical money.

We have adapted marvelously, and even after the lockdown measures are no longer applicable, we will keep, to a large extent, to our newly acquired habits.

> Pandora's box has been opened. This means that the way markets function will never be the same again

Pandora's box has been opened. This means that the way markets function will never be the same again, since the looming threat of a pandemic will always be relevant, and since both customer and personnel expectations have already grown accustomed to the convenience of electronic transactions and remote working. And while this universal remote working environment has opened a world of possibilities and opportunities, it is not free of inherent risks.

With this monumental yet sudden increase in remote working environments, the cyber-threat landscape stands drastically changed. From a cybersecurity point of view, the arena has forever been altered. Organizational networks and the devices connected to them have expanded well beyond the confines of their cyber defense network perimeters, this way widening their cyberattack surface to a variety of cyber-threats and vulnerabilities that were not previously relevant to most organizations. This provides opportunities for ambitious cybercriminals to exploit the increase in cyberattack targets, as well as the inexperience of some organizations with conducting business via such a hybrid model in a secure and confidential manner.

Already, cybercrime activity has surged in recent weeks, with threat actors adopting creative methods of taking advantage of the fear surrounding the pandemic, and so tricking users into downloading malicious software or clicking on seemingly benign links that in reality can compromise their workstations. Examples of coronavirus-inspired cyber-attacks are emails from supposed N95 mask suppliers who promise fast deliveries to those who follow a provided link or who download a shady attachment.

Such social engineering and phishing methods generally aim to gain access to a workstation outside of the organizational network, this way escalating access privileges for threat actors who will then use them to conduct data breaches for the theft of valuable information, the disruption of their target's business continuity, and the damaging of their reputation.

Alternatively, targeted cyberattacks may be conducted with Man-In-The-Middle attacks, through which a threat actor can intercept a remote worker's wired/wireless communications and either eavesdrop or falsify the digital communications being transmitted. Since we now rely heavily on working remotely and making online transactions, we are more and more exposed to increased risk of identity theft, fraud and even monetary theft.

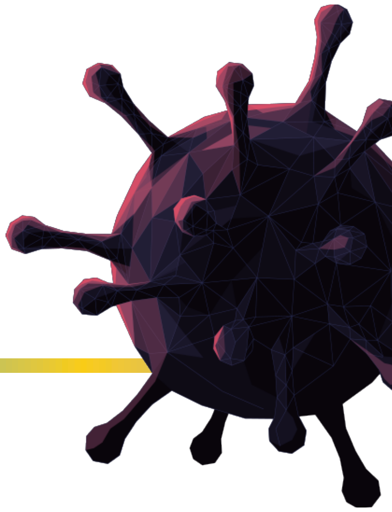
> **Since we now rely heavily on working remotely and making online transactions, we are more and more exposed to increased risk of identity theft, fraud and even monetary theft.**

What is alarming is that most organizations and their people are not accustomed to utilizing the internet for their everyday tasks. This means that cyber awareness and cybersecurity good practices need to be adopted among remote workers as fast as possible before their recently expanded organizational networks become exposed to targeted cyberattack campaigns.

There is, however, much we can do to timely adapt to this ever-changing threat landscape. We can remain vigilant when it comes to the security precautions we apply to safeguard our people, their home workstations, and our organizational networks in general. We need to educate our people on social engineering and cybersecurity best practices, to elevate their awareness when it comes to the contemporary reality of cyber-threats and vulnerabilities. We can then adopt additional security layers, stricter password policies, restricted access privileges, and integration of comprehensive cybersecurity solutions on an organization-wide scale. Taking it a step further, we can engage in Managed Security Services to drastically reduce the possibility of cyberattacks, data leakages and cyber fraud. Finally, we should tie our technological adaptations with enhanced organizational governance parameters (procedures, processes, policies, protocols) for a well-rounded security approach that is up to date and in accordance with an ever-expanding cyber-threat landscape.

History proves to us time and again that humans are highly adaptable when responding to shifting circumstances. We will beat this pandemic, and we will address the elevated cyber risk that stems from social distancing and the inevitable expanded cyberattack surface that remote working has created.

STAY SAFE AND STAY
CYBER SECURE.



HEADQUARTERS

CYPRUS
1 Lefkos Anastasiades Str.2012 Strovolos, Nicosia

T +357 22463600
F +357 22463563
E info@odysseycs.com

www.odysseycs.com

ODYSSEY™
cybersecurity

OFFICES CYPRUS | GREECE | USA | UK | KSA