Cyberattacks increase as WFH continues

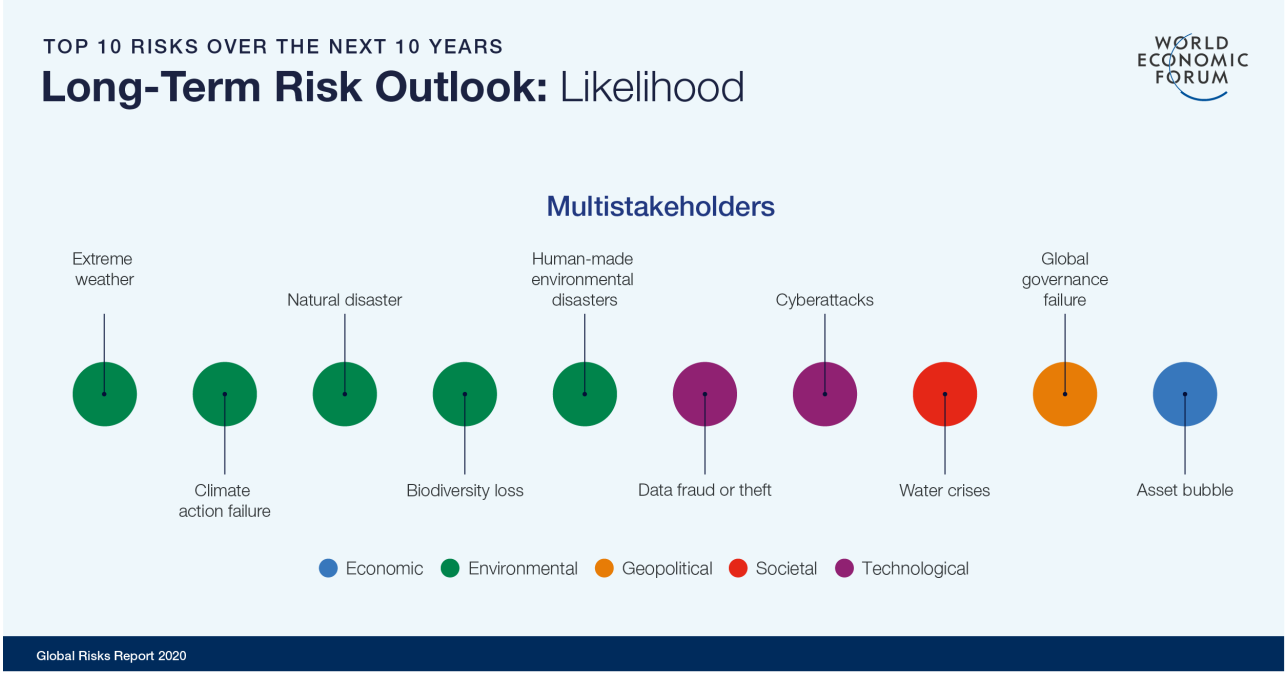
According to research conducted by the World Economic Forum, cybercriminals are using the time during COVID-19 lockdown to launch cyberattacks.

Temps de lecture : minute

9 May 2020

The latest research from the World Economic Forum on Global Risks shows the impact of COVID-19 crisis on the global economy weakens cybersecurity and encourages hackers to cyberattacks. Now more than ever, companies across the world with teams working from home need to strengthen their protection and shield their IT solutions.

People around the world are totally dependent on their organisation's digital infrastructure, and they need to be made aware of the risks, to be trained accordingly on the use of specific tools and to be confident that they are protected while working online. Otherwise, their equipment is at risk in the long term, in times when cybercriminal activity is growing due to the global dependency on the Internet, which is such a critical tool for business.



> *"There has been a significant growth in cyber criminality in the form of high-profile ransomware campaigns over the last year. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud, while lives were put at risk and services damaged by the WannaCry ransomware campaign that affected the NHS and many other organisations worldwide. Tactics are currently shifting as businesses are targeted over individuals and although phishing attacks on individuals are increasing, fewer are falling victim as people have become more alert." - UK National Crime Agency*

To palliate the risks of cyberattacks and data theft that cost global businesses billions each year, experts in cybersecurity offer their support

with revolutionary IT solutions to reinforce their clients' digital infrastructure. In light of soaring threats amid the outbreak, a London-based cybersecurity startup, swIDch, decided, as of April 27, to provide a 3-month free trial of its *OTAC (One Time Authentication Code)* to support businesses manage their employee access management more securely.

What is "OTAC"? It's a one-time authorisation code, meaning a code that is valid to authenticate a user's identity for one session only. Not only is it used in mechanisms to identify a user's identity, but also in the computing sector. Someone using a desktop or laptop for a web application might use an OTAC to securely authenticate with the web application.

> *"As a cybersecurity startup, we came up with a resolution to defeat another terrible virus on your computer in a manner fitting the current circumstances." - Chang-hun, Founder of swIDch*

So, swIDch offers OTAC technology to enable employees to generate a one-time dynamic authentication code for access management. This method can generate unique dynamic codes even in an *off-the-network* environment, eliminating the attack surface for hackers. The codes are enough to identify a user on its own, therefore the businesses do not rely on the use of other technologies, saving costs for them. Thanks to this solution, swIDch aims to reduce fraud and data theft and reduces the risks of cyberattacks for companies.

Article écrit par Audrey Langevin