IS HOME WORKING HERE TO STAY?

Coronavirus has changed the way many employees work – and companies need to adapt their IT security accordingly, says NCP's Patrick Oliver Graf.

THIS YEAR HAS BROUGHT MANY UNEXPECTED DEVELOPMENTS AND SETBACKS FOR COMPANIES of all sizes and industries – some with far-reaching operational and economic consequences. Now it's time to take stock and consider some key questions. Why are cyber risks above all business risks? How prepared were companies for the changing world of work in 2020? What can we learn for the future? In this interview, NCP Managing Director Patrick Oliver Graf reports on the frontline experience his company has made in 2020, and shares insights into the current situation.

Will the Coronavirus pandemic have lasting changes on the world of work?

PATRICK OLIVER GRAF: The situation since the beginning of the year can certainly be described as a stress test for digitalization. Some companies were already in a good position to switch their workforce to working remotely from home with relative ease. Others were not so well prepared and could not obtain the necessary hardware due to supply shortages and dependency on international suppliers. Within a very short time, allowing employees to work from home became vital to business continuity, rather than just a perk for employees.

Will those employees who are working from home because of Coronavirus continue to do so when the risk has receded?

PATRICK OLIVER GRAF: As the Coronavirus pandemic continues to affect our lives, working from home is likely to prevail in the long-term for employee protection alone, although many companies have also seen the benefits of enabling a remote workforce. This will certainly make the world of work much more flexible. In recent weeks, companies such as Siemens have already announced that their strategy is to enable employees to work two-to-three days a week from home in the future. Telefónica Deutschland wants its employees to be completely free to decide when and where to work.

> The impact of Coronavirus can certainly be described as a stress test for enterprise digitalization.

COMPANY INFO | NCP ENGINEERING GMBH – IT SECURITY MADE IN GERMANY

NCP engineering is based in Nuremberg, and has provided 'IT Security Made in Germany' for more than 30 years to customers around the world. As a specialist in secure communications for companies of all sizes and industries, NCP engineering is currently on the front-line of a world that is rapidly transitioning to remote working.

DETAILS
To find out more about NCP engineering please visit:
🌐 | **ncp-e.com** ✉ | **info@ncp-e.com**

A global pandemic does not happen every day. Can companies really be expected to prepare for these exceptional situations?

PATRICK OLIVER GRAF: Even before the pandemic, other incidents have made it necessary for employees to work from home. Hurricane Sabine in Germany and Central Europe at the beginning of the year, heavy snowfall, natural disasters or chemical mishaps – all are examples of incidents that can prevent employees from coming to the office to work. And it is important not to overlook manufacturing processes – production plants that have already implemented secure remote maintenance have made a wise decision.

What should companies learn from the situation?

PATRICK OLIVER GRAF: Companies are generally at an advantage if they are flexible and can scale the solutions they use up or down to match the current demand. Ideally, they would only pay for what they use like the pay-per-use models that we have long been accustomed to in the consumer sector. Companies need to understand that securing external access to the company network via VPN is an important means of maintaining business continuity, beyond being an important part of cyber security strategy. Flexible remote working is, in many cases, the only way to keep operations running in 2020.

What are the cyber risks associated with working from home?

PATRICK OLIVER GRAF: Companies are currently under pressure to provide secure work equipment, but also to raise their employees' awareness of cyber security issues. Data protection and privacy laws play an important role here, and companies and their employees need to be acutely aware of the implication of these laws on the data they are processing. Adapting the company's network infrastructure and cyber security strategy to allow employees to work from home poses complex challenges, but these generally already apply to remote working, even when employees use their laptops in hotels and airports when traveling for business.

Are there any solutions and best practices that companies could consider?

PATRICK OLIVER GRAF: Yes, there definitely are solutions and best practices to be considered. In comparison with the BYOD (Bring Your Own Device) model, companies that provide devices for their employees to use are in a better position to manage security. Today, very granular access to the corporate network can be configured, with a focus on strong authentication as well as automated monitoring of connected systems – e.g., verifying that the Operating System and virus scanner are up to date, to name just a few examples.

> Even before the pandemic, other incidents have made it necessary for employees to work from home.

Are there positive lessons to be learned from the current situation?

PATRICK OLIVER GRAF: The Coronavirus pandemic has certainly put its finger on the sore spot of globalization and digitalization, but this, in the long term, will ensure that the impact of IT security on business objectives is much better understood by decision makers.

Patrick Oliver Graf (pictured, right) is CEO & Managing Director at NCP engineering GmbH.