Fortifying your remote working conditions

May 2020

As the world contends with the COVID-19 pandemic, organizations are being forced to adapt quickly to novel methods of working. The rapid conversion of on-premises business operations to remote working conditions has exposed many companies to numerous risks – many of which are being exploited by organized crime groups, hackers and criminal opportunists. Could you imagine the implications of a cyber attack while your staff and customers are stuck at home? How much longer can your business bear the cyber risk of the threats brought about by the COVID-19 pandemic?

Five key risk areas to focus on:

The following key risk areas triggered by the rapid conversion of on-premises business operations to remote working conditions, can expose a business to criminal opportunists through a number of ways. These are but a few examples.

Insecure Remote Access

due to ineffective authentication, encryption and lack of capacity

Insecure remote workplace environments

due to reduced levels of controls in remote and unvetted – yet trusted – working spaces which can expose your company to data leaks and data loss

Insecure or unauthorized use of cloud services and collaboration tools

such as shadow IT, insecure web conference tools, and the inappropriate use of data sharing tools

Supplier disruptions

such as business process outage due to insufficient capacity of communication service providers

Slow or no response time for handling security incidents

because key IT staff are working remotely and can't access company IT systems in a timely manner

Understand Digital Footprint → **Assess Key Controls** → **Develop Remediation Roadmap** → **Report**

With a four-phase process, you gain short term and medium term actions to minimize your exposure to risks while your teams are working remotely – and you lay the groundwork for working safely in the new normal.

How can we help?

KPMG provides you with a clear understanding of your risk exposure with a gap assessment and an actionable remediation roadmap for key controls in the following nine areas. You can expect this service to be delivered within three to four weeks.

Secure remote connectivity	**Secure remote collaboration tools**	**Mobile device hardening**
Corporate laptop security	**Secure cloud workloads**	**Crisis plans on supplier disruption**
Awareness and training to secure remote working	**(Remote) security incident management**	**Compliance with privacy and security regulation**

Your benefits

- ✓ **Peace of mind** with a clear understanding of your company's cyber risk exposure as a result of rapidly changed work environment and increased levels of cyber threats
- ✓ **Confidence** in knowing you are doing the right thing to protect your organization from cyber attacks – and that you have laid the groundwork for a more stable, more secure, cyber infrastructure that will help you master the COVID-19 crisis and be ready you for the new normal.
- ✓ **A greater sense of security**, because you know your staff is better enabled and empowered to do their jobs without the fear of exposing your company to a cyber attack
- ✓ **Clear sense of direction** thanks to a focused and actionable remediation roadmap to mitigate the cyber risk, including quick fixes

Find additional KPMG COVID-19 resources here

https://home.kpmg/ch/en/home/insights/2020/03/coronavirus-business-continuity-plan.html
https://home.kpmg/ch/en/home/insights/2020/04/coronavirus-increased-forensic-and-cyber-risks.html

Contacts

KPMG AG
Räffelstrasse 28
PO Box
8036 Zurich

kpmg.ch

Dr. Matthias Bossardt
Partner, Head of Cyber Security Consulting
+41 58 249 36 98
mbossardt@kpmg.com

Yves Bohren
Director, Cyber
+41 58 249 48 95
ybohren@kpmg.com

Dr. Thomas Bolliger
Partner, Cyber
+41 58 249 28 13
tbolliger@kpmg.com

Nicolas Tinguely
Director, Cyber
+41 58 249 21 44
ntinguely@kpmg.com

Fortifying your remote working conditions May 2020