Cyber Security

Work anywhere, together

The COVID-19 pandemic delivered a seismic shock to most organizations' working models. In the rapid shift to remote work, the usual checks on security and privacy controls took a back seat. Working anywhere has exposed many companies to reputational and compliance risks with cyber threats mounting as organized crime groups, hackers and criminal opportunists take advantage.

It's also more difficult now to remain secure with so much of the intellectual property and activity happening in decentralized locations. Moreover, businesses are having to remain compliant across different jurisdictions with differing regulations on data privacy and intellectual property. It's crucial for companies to have clear and consistent procedures and policies to minimize all of these risks, while still offering the flexibility employees seek.

Your challenges

The following key risk areas triggered by the rapid conversion of on-premises business operations to remote work conditions, can expose a business to criminal opportunists in 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 a reduced level 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 an 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.

How KPMG can help you

With our four-phase process, you gain short- 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.

Understand digital footprint → Assess key controls → Develop remediation roadmap → Report

We provide 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:

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

You can expect this service to be delivered within three to four weeks.

Your benefits

- **Peace of mind** with a clear understanding of your company's cyber risk exposure as a result of a rapidly changing 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 prepare you for the new normal.
- **A greater sense of security,** because you know your staff is better enabled and empowered to do their job 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.

Contact

KPMG AG
Räffelstrasse 28
PO Box
8036 Zurich

kpmg.ch

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

Thomas Bolliger
Partner Information Management and Compliance
+41 58 249 28 13
tbolliger@kpmg.com

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

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