KPMG

Cybersecurity during Covid-19

Pivoting to remote working at scale

May 2020

Covid-19 has driven radical change in businesses. Your offices are empty, your business is under pressure and your employees are adapting to the new mode of working. How do you ensure your security is scaling with your remote working infrastructure?

The efforts to manage the Covid-19 pandemic have forced enterprises to rapidly adapt to new working models. At the heart of this is a complex and fast changing web of digital infrastructure. As IT teams scramble to implement changes within weeks that before might have taken years, security teams need to be an enabler, not a blocker to change.

Shine a light on shadow IT infrastructure

Your business team leaders and employees need ways to communicate and collaborate when they can't be in the office together. Many will ask for digital solutions you've not approved as a team.

Embrace those solutions. Encourage the business to purchase enterprise licenses for those solutions and be part of the procurement and digital integration discussions. Help roll out those solutions, but make sure security advice and secure configurations are in place to help manage access, functionality and data loss prevention controls. If you don't, they will happen anyway, and you'll have shadow IT issues.

Access controls are more critical than ever

Multi-factor authentication or at least strong password controls are essential for remote access to enterprise IT systems. Also, consider conditional access/CASB solutions which allow you to limit access to your enterprise systems to those corporate devices or BYOD with an endpoint or mobile device management solution in place. Strong passwords or passcodes are also important for end-user devices.

Ideally, encourage staff to separate their personal and work activities using different devices, unless you are forced to adopt BYOD solutions.

Multi-factor authentication should be in place for all privileged access. However, you should also ensure that delegates are in place and where necessary "break glass" arrangements if key individuals are not available. Don't just assume a single delegate is sufficient.

Keep up your data loss prevention controls

Data loss prevention helps to both preserve enterprise IP and uphold legal personal data privacy requirements. Ensure that MDM tooling and endpoint DLP solutions are suitable for remote working at scale, and explore options for managing personal devices if they must be used for business purposes. Disable or restrict access to insecure home printers, monitors and removable media devices. Do staff really need USB media access at home?

Keep your employees informed about threats

Malicious actors and threat groups are exploiting the Covid-19 pandemic by deploying tailored phishing campaigns. These campaigns target employee or business financial assets. They attempt to solicit account credentials or release malware (including ransomware) onto enterprise networks.

Follow threat updates from reliable threat intelligence sources and ensure these are communicated to your employees regularly as an integral part of your Covid-19 communications strategy. Help staff to recognize phishing scams. Ask employees to report suspicious emails or files (and make it easy for them – ideally, a single button on your email client). Share what you see with the security community; everyone is at risk.

Put your security operations on guard

Threat groups are exploiting the enormous workload on IT and security teams, and are launching enterprise-level ransomware attacks, crypto-mining operations and denial of service attacks. Security operations center (SOC) and disaster recovery teams may not be used to, or able to, work remotely or with only a few members on-site at a given time. Now more than ever, detection and rapid response to cyber threats matter.

Ensure adequate staffing, and that staff members are well-practiced in handling attacks whilst working remotely. If staff need to come into work and might be questioned by authorities for doing so, provide them with a letter of authority confirming their importance to your organization.

Put in place and test alternative measures to communicate with and access data centers, restore systems from physical backups, and failover/failback to resilience servers. For events that escalate, ensure that you have back up communications systems for incident response teams. Most importantly, ensure you have deputies for key personnel in business continuity and crisis management teams, in case team members fall ill or are unavailable due to travel restrictions.

Deal with wear and tear

It's not possible to be sure how long employees will be out of the office; during this time, employees will have issues with IT systems and work devices. If you're used to on-site IT teams managing issues with employees' devices and systems, consider how to facilitate phone assistance or remote management of devices securely. Put in place mechanisms and guidance to allow faulty IT equipment to be securely returned for maintenance, and new IT equipment to be shipped and securely configured.

Monitor your employees' cyber hygiene

Recognize that your employees are working in unfamiliar ways with unfamiliar systems. Encourage them to seek help if they are unsure and avoid a culture of blame. Line managers need to keep in touch with their teams to build team spirit and watch out for employees who may be feeling isolated or may be acting in ways that raise concerns.

Ensure employees also have ways to raise concerns over working practices, helping IT and security work to securely facilitate their roles and pre-empt "workarounds," which may cause security issues.

Sanity check your privileged users

For employees with privileged business access or system administrative rights, regular chats can help identify any stress or other behavior issues that raise concerns. They can also improve their wellbeing, team relations and productivity.

Assess your remote access capability

Organizations recently moved to remote working due to Covid-19 leading to potential cybersecurity risks. Access your Remote Access Capabilities, and ensure acquired systems allows you to access your data safely.

Look after your joiners, movers, leavers controls

Organizations are facing financial pressures during this period, leading to potential redundancies among staff and contractors. In other areas, organizations may be on-boarding emergency third party support, building team capacity for critical processes, or restructuring teams to support other business units and roles.

Security teams need to work closely with HR and IT to manage the high volume of joiners, movers and leavers through the organization. All of these processes need to be performed remotely, and you will need to agree on approaches to securely provision accounts quickly, even if you need to manage risk by limiting access initially.

Given the absence of personnel and supervision of the office space during remote working, activities such as revoking physical access cards are particularly important.

Reach out to the community

Surviving the Covid-19 pandemic requires businesses to reach out to peers, regulators, trusted partners and supply chain contacts to improvise novel solutions. Work with your ecosystem; share your experiences and ensure you are well supported. This is a time of stress for everyone, as we all try to be superheroes.

Feel free to contact us if you have any questions, or would like support or advice.

Contacts

Tariq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393