KPMG

COVID-19

How secure are your remote working arrangements?

April 2020

As the world contends with the COVID-19 pandemic, organizations are being forced to rapidly adapt to novel methods of working. They are grappling with the challenges of working from home and business continuity sites, under highly restricted conditions. In response to the disruption, many companies across the region have enabled remote access solutions, remote collaboration tools, and cloud services. Several are allowing employees to use personal devices and have enabled the use of home networks for an extended period of time.

Some organized crime groups have recognized an opportunity to exploit the seeds of fear and uncertainty sown by COVID-19, and take advantage of the control deficiencies associated with remote working conditions, to target individuals and businesses in a variety of ways. KPMG has identified key controls across ten risk areas.

How secure is your remote connectivity?

Remote access policy awareness	Have you established user guidelines and security best practices related to remote access?
Privilege management	Have you assigned remote access privileges to users based upon specific business roles?
Secure and encrypted access	Does your remote access system enable you to configure the highest standards of security protocols (e.g. Point-to-Point Tunneling Protocol (PPTP), Layer Two Transport Protocol (L2TP))?
Network traffic filter	Are you able to restrict network traffic based on specific protocols and port numbers?
Two-factor authentication	Have you enabled at least two-factor authentication on your remote access systems? (Note: A multi-factor authentication (MFA) system will provide you better security.)
Vulnerability management	Do you have a vulnerability management process to regularly check for vulnerabilities and patches, along with firewall protection for remote access employee devices?

Security monitoring	Have you set up strict monitoring for remote users' audit logs, administrative logs and transaction logs?
Split tunneling	Have you disabled split tunneling for remote users connected through the corporate VPN?
Bandwidth assessment for VPN	Did you perform pre-stress checks to ensure your VPN bandwidth is adequate to handle a large number of VPN connections?
Corporate perimeter security on remote access	Have you enforced remote user connections to terminate on a perimeter device that is segregated from the internal networks?

How secure are your remote collaboration tools?

Governance controls	Have you defined adequate governance over the usage of collaboration tools (e.g. file retention policies, deletion of messages and content retrieval)?
Access to tools	Have you provided access to collaboration tools via thick clients instead of browsers to prevent browser-based attacks?
VPN-based access	Have you enabled access to collaboration tools only via corporate VPN? Have you enforced MFA to access VPN?
Generic URL	Are organizational links on browser-based access set to generic names, instead of names that may reveal internal details (e.g. companyname.app.com)?
Disabling of auto previews	Have you disabled auto preview of images shared via links on collaboration tools to avoid leaking of device IP over the network?
Disabling hyperlinks	Have you enforced policies to disable hyperlinks via instant messages to reduce phishing attempts?
Identity and mobility management	Have you configured collaboration tools with adequate identity and mobility management controls (such as SAML authentication, SSO, Enterprise Mobility Management) along with integrity checks of installed applications?
Data security	Have you enabled adequate data security controls in collaboration tools, such as restricted sharing of documents internally as well as externally, blocking of unmanaged device access using DLP, etc.?
Logging and monitoring	Have you configured logging and monitoring controls for each collaboration tool to manage incidents and investigations with respect to file download/upload, unauthorized access attempts, etc.?
Training and security awareness	Have you trained your employees on the use of collaboration tools and the associated security considerations? (e.g. who can be invited to group meetings/conferences?)

Have you configured adequate security on mobile devices?

MDM solution	Are you using a mobile device management (MDM) solution to manage personal devices and corporate-owned devices with access to corporate data?
User authentication	Have you configured strong user authentication such as screen lock password/PIN for devices with access to corporate data?
Key user settings	Have you configured key security settings such as disabling autofill, enabling automatic device lockout, and allowing apps to only be installed from trusted app stores?
Anti-theft measures	Have you configured anti-theft measures such secure remote wipe in BYOD and corporate-owned devices?
Storage encryption	Have you enforced encryption of storage media in the mobile device so that corporate information residing in the device cannot be accessed if the device is stolen?
Anti-malware protection	Have you configured an anti-malware solution on BYOD and corporate-owned devices to protect against malware?
Security updates	Are you sending notifications to all employees to ensure they keep their mobile devices updated with the latest security patches? Have you configured over-the-air (OTA) distribution features to push security and other software updates remotely?
Outdated OS restrictions	Are you ensuring that older versions of iOS and Android operating systems are not allowed to access corporate resources?
Rooted device restrictions	Have you configured policies on your MDM to check for jailbroken/rooted devices to ensure they are not allowed to access corporate resources?
Connection security	Have you ensured that external connections to the device (such as Wi-Fi, Wi-Fi Direct, Bluetooth, Hotspot, USB, USB OTG) are restricted and/or secured adequately?
Data backup	Is critical data residing on mobile devices being backed up regularly?

Have you configured adequate security on corporate laptops?

Least privileged accounts	Have you restricted the use of administrative accounts to only a few staff, based on their business roles?
Strong account policy	Have you configured a strong password policy in all company provided laptops (e.g. complex password, minimum length of 8-12 characters, minimum/maximum password age, etc.)?
Password protected screensaver	Do you enforce password protected screensavers in all company provided laptops?

VPN-based remote access	Have you configured access to corporate applications so they require company provided VPN connection?
End-point security solutions	Have you deployed end-point security solutions e.g. anti-virus and DLP (data loss prevention) solutions in all company provided laptops?
Removable media restrictions	Do you restrict the use of removable devices, such as USB devices, to prevent duplication of corporate data?
Hard disk encryption	Have you enforced hard disk encryption in all company provided laptops using solutions (e.g. bit locker) and pushed this as a security measure during OS start-up?
Regular backup	Does your corporate IT policy enforce regular data backups from all company provided laptops via online data backup solutions?
Webcam cover	Have you provided web cam covers for all company provided laptops to ensure that employee privacy is safeguarded from unintended video capture via trojans?
Physical cable locks	Have you provided Kensington cables for all company provided laptops in order to physically secure company equipment and data?

How secure are your workloads on cloud?

IAM: Authentication	Are you protecting your cloud workloads using multi-factor authentication (MFA/2FA)?
IAM: User access control	Have you implemented access controls that ensure only authorized users access cloud data and applications?
IAM: Privileged access	Have you implemented additional controls to secure privileged access e.g. conditional access control, just in time, etc.?
IAM: Malicious behavior identification	Can you detect compromised accounts and insider threats to avoid malicious data exfiltration?
Information protection: Data classification	Do you have a data classification and handling policy to make sure only permissible data is allowed to go into the cloud workloads?
Information protection: Data loss prevention	Have you implemented a cloud DLP solution to protect data from leakage, based on your data classification schema?
Information protection: Encryption	Are you using cloud data encryption to prevent unauthorized access to data, even if that data is exfiltrated or stolen?
Network security: Perimeter	Have you implemented adequate perimeter security controls e.g. DODS protection, WAF, Firewall, etc.?

Network security: Segregation	Have you implemented adequate network segregation grouping to ensure only permissible traffic between cloud workloads?
Network security: Secure protocols	Are you using secure protocols at the network (e.g. TLS) and application layer (e.g. IPSEC, SSH, SSL) while accessing cloud workloads?
Advanced threat protection	Have you configured advanced threat protection controls to identify suspicious user and device activity with both known-technique detection and behavioral analytics?

How are you going to remotely supervise high risk processes?

Sensitive operations planning	Do you have documented procedures to manage sensitive operations remotely e.g. cash management, loan processing, wire transfers, call center, etc.
Access to critical systems	Have you made sure only authorized business users and administrators have remote access to carry out critical business processes such as reconciliation, customer operations, etc.?
Maker and checker	Have you defined a monitoring mechanism to ensure maker and checker controls are operating effectively in remote working conditions?
Privileged access management	Are you using a privileged access management (PAM) solution to control remote activities of users with administrative privileges?
Unavailability of staff	How would you ensure the maker and checker controls in the event of a significant level of absenteeism?
Change authorization	Do you have a change authorization workflow defined to prevent unauthorized modifications to the production environment and critical processes remotely?
Systems unavailability	Have you established and communicated alternate processes to be followed by employees if primary systems are unavailable?
Data leakage prevention	Have you implemented a DLP solution to protect data from leakage by users working remotely on high-risk processes?
Fraud monitoring	Are you using any fraud monitoring system to detect and deter fraud?
Security monitoring	Have you implemented a cyber security monitoring system to perform real-time analysis of cyber security alerts and manage cyber security incidents?

Can your supplier's disruption affect your crisis plans?

Geographic restrictions	Do you have visibility of your entire supply chain in order to anticipate regional disruptions that may impact your continuity efforts?
Supplier continuity	Have you discussed with your key vendors and suppliers how their crisis plans will support your continuity efforts?
Supplier point of contact	Have you established the point of contact and mode of communication with your key vendors and suppliers that can be used in case of an emergency?
Supplier remote working capabilities	Have you assessed your key vendors' and suppliers' capability of to support remote working (e.g. online collaboration tools, video-audio conferencing, cloud based solutions)?
Contractual provisions for emergency	Do your existing contracts and relationships with key vendors and suppliers allow requests for additional capacity and support in case of an urgency?
Alternate vendors and suppliers	How will you manage your operations if your key vendors and suppliers are disrupted due to the evolving situation? Have you thought about diversifying vendors and suppliers?
Additional equipment needs	How will you address requirements to procure additional equipment that you may require to support the remote working conditions?
Stockpile of key equipment	Do you have stockpile of key equipment that you may require to support remote working conditions e.g. additional laptops, mobile phones etc.?
Dependency of vendors and suppliers	Are there steps that you can take now to reduce that dependency, including using your own resources?
Short-term and-long term plans	Do you have short-term (return of normalcy in a short span) and long-term (prolonged pandemic situation) plans to handle supply chain disruptions?

How are you protecting your workplace environment from infection?

COVID-19 infection plan	Have you established and communicated a comprehensive infection plan to employees to handle the COVID-19 pandemic?
Awareness	Are there proper respiratory and hand hygiene guideline posters around the workplace?
Personnel safety	Are employees told to stay home and immediately consult a doctor in case of any symptom in order to minimize the spread of COVID-19?
Thermal camera	Do you have perimeter safeguards, such as thermal cameras and masks, for visitors before allowing them inside the workplace?

Temperature monitoring at workplace	Is your office equipped with handheld thermometers to measure employees' temperatures in the workplace?
Area and surface cleaning	Are workplaces, pantries, restrooms and frequently touched surfaces such as doorknobs, countertops, light switches, elevator buttons regularly cleaned?
Proper ventilation	Are the ventilation, air purification and air conditioning (HVAC) systems working properly in your workplace?
Hygiene products	Are employees provided with proper hygiene products, such as hand sanitizer, tissue paper, facemasks and gloves?
Workspace cleaning	Are the desks and computers used by employees cleaned with disinfectant on a regular basis?
Waste disposal	Are waste products disposed of frequently and in a hygienic manner?

Are you effectively communicating to secure remote working conditions?

Remote working policies	Have you communicated the changes in information security policies due to current remote working conditions?
Communication plans	Do you have clear communication plans in place to manage internal and external communications related to cyber security incidents? Have you provided relevant contact information to your employees/customers in case of any security breaches?
Communication infrastructure	Have you put official communication channels in place to support remote working conditions?
Crisis management team	Have you established an internal crisis management team, including senior leaders in pivotal positions?
Disinformation	How are you verifying news related to COVID-19 before circulating or acting on the information?
Phishing attacks	Have you conducted refresher sessions for employees on the recent forms of phishing emails that use the COVID-19 scare as a lure?
Imposters	Have you raised awareness among employees that imposters may reach out through phones or at your doorstep posing as government officials requesting their personal data?
Remote working safe practices	Have you conducted refresher sessions on best practices for remote working e.g. not using public Wi-Fi, physically securing unattended equipment, not using office laptops for personal work, etc.?

Data Handling	Have you given employees clear guidance as to how information should be handled when working remotely?
Customer bulletins	Are you communicating with your customers about safe Internet practices and the latest COVID-19 related cyber threats?

Do you have plans to respond to specific cyber/information security incidents?

New COVID-19 threats	Is your security operations center (SOC) continuously monitoring the latest cyber threats e.g. new 600+ domains related to COVID-19 that have been registered globally?
Incident response plan	Have you updated your incident response plans to cover the latest cyber security threats that are prevalent due to work-from-home conditions e.g. targeted phishing emails, ransomware, DDOS of VPN devices, etc.? Have you tested the plans?
Incident response governance	Have you established adequate governance mechanisms to manage cyber security incidents, considering the pandemic?
Alternate SOC arrangement	Have you evaluated the need to look for alternate arrangements for the SOC, considering the current pandemic e.g. loss of key MSSP resources, lack of adequate network bandwidth from MSSP, etc.?
Incident reporting channels	Are employees aware of appropriate channels for reporting cyber/information security incidents that they may identify while working from home?
Laptop and mobile device incidents	Do your SOC monitoring and incident response plans cover the end user's equipment? (e.g. laptop and mobile devices)
Cloud service incidents	Do your SOC monitoring and incident response plans cover the cloud workloads?
Remote collaboration tool incidents	Do your SOC monitoring and incident response plans cover remote collaboration tools?
Cyber investigations	Are there procedures in place to identify, collect, and preserve cyber security incident data from end user's equipment while working from home?
Incident recovery	Do you have adequate recovery arrangements in place to restore impacted services on a timely manner, as per business requirements?
Post-incident review	Do you perform post-incident reviews and document lessons learned to prevent reoccurrence of similar incidents?

Contacts

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

home.kpmg
home.kpmg/socialmedia

kpmg.com/sa

Follow us on:

Designed by KPMG Lower Gulf Creative team.

Publication date: April 2020