Information on Safe Home Working During the COVID-19 Pandemic

Updated 20 March 2020 version 1.3

The following provides a description of recommended security procedures for remote working, whether via remote access or local. It is intended as a guide only rather than a definitive set of procedures. Security will also depend on the type of content i.e. a feature film tent pole title or a TV episodic and we believe the default guidelines about remote and home working must be directed by content owners. Once this has been established the following security measures are recommended for each scenario in addition to MPA Best Practices (which cover some but not all instances for remote working).

Introduction

- Share safe home working practices relevant to your situation
- Based on MPA Best Practices & Content owner guidelines
- Input by senior security assessors: Nik Savchenko, Ben Bradley, Tony Ramsay (Convergent Risks).
- Created in collaboration with content owners

Types of Home Working

- Non-local (e.g., VPNs and Remote Desktop)
    - Vendor
    - Home Worker
- Local (content is hosted on site, e.g., encrypted hard drive)
    - Remote location
    - Home Worker

Types of Home Working (expanded)

- Remote access to onsite workstations (hosted within the facility) through an onsite bastion host server (i.e. VPN, SSL, SSH keys, 2FA etc)
- Remote access to onsite workstations (hosted within the facility – hardware offsite) through a PCoIP KVM solution (i.e. Teradici)
- Remote access to onsite workstations (hosted within the facility – hardware offsite) through a proprietary hardware/software/network solution (i.e. sohonet Clearview)
- Remote access to cloud-based hosted production operations/content (i.e. StratusCore, BeBop, VM etc)
- Content accessible offsite and worked on company hardware/personal network point – i.e. company hardware shipped and installed in offsite

location (downloaded via content transfer servers/web-based file transfers or provided on portable hard drive)
- Content accessible offsite and worked on personal hardware/personal network point (downloaded via content transfer servers/web-based file transfers or provided on portable hard drive)

Essentials for 'Safest' Home Working with Content

- Encrypt
  - Download content via approved method to encrypted hard drive
- Disable
  - Disable all network connections (wired and wireless) whilst accessing the content on the hard drive
- Reconnect
  - Only reconnect the workstation to the Internet to transfer content back to the client/vendor or if the hard drive has been disconnected

1. The Basic Essentials for Home Working (Non-local):

- Vendor:
  - Prohibit direct remote access to the content / production network without the use of an approved bastion host model
  - Remote access accounts must not be shared
  - Maintain a list of company personnel who are authorized for remote access to the content /production network
  - Develop processes for management to review remote activity and monitor access to systems that reside on the content / production network
  - Configure remote access systems to use individual accounts
  - Limit remote access to a single method with Access Control Lists
  - Use two-factor authentication, and preferably certificate based
  - If possible, block file transfer protocols including, FTP, SSH, IRC, IM
  - VPN configuration must not allow split tunnelling
  - Perform on at least an annual basis, penetration testing of all external IP ranges and hosts and remediate issues.
  - Conduct monthly vulnerability scans of external IP addresses
  - If possible, only allow users to work from specific IP addresses (i.e., home not a coffee shop)
  - Capture and retain all logs pertaining to remote access. Regular review of logs should also be conducted

- Home worker:
  - Only use wired connections where possible
  - Disable WiFi capability on workstation/laptop
  - Ensure default username/password (including administrative access) is changed on ISP provided wireless router
  - Workstation/Laptop must have full disk encryption applied
  - Implement use of privacy screens
  - Install and maintain up to date anti-virus on workstations / laptops
  - Do not store content on workstations / laptops
  - Do not use public WiFi networks

- Ensure screens/monitors displaying content do not face windows (Blinds and curtains can also be deployed).

2. The Basic Essentials for Home Working (Local):

- Vendor:
    - For digital transfer, use only client-approved transfer systems that utilize access controls, a minimum of AES-256 encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.
    - For physical transfer, encrypt content on hard drives or encrypt entire hard drives using a minimum of **AES-256 encryption** by either:
        - File-based **encryption**: (i.e., encrypting the content itself)
        - Drive-based **encryption**: (i.e., encrypting the hard drive)
    - Capture and retain all logs pertaining to content transfer. Regular review of logs should also be conducted
- Home worker:
    - If Internet connection is required for download/upload purposes, only use wired connections where possible
    - Disconnect workstation/laptop from Internet (wired and wireless) when accessing content on physical media
    - Disable WiFi capability on workstation/laptop
    - Ensure default usernames/password (including administrative access) are changed on ISP provided wireless router
    - Workstation/laptop must have full disk encryption applied
    - Implement use of privacy screens
    - Do not store content on workstations/laptops
    - Do not use public WiFi networks
    - When not in use, secure hard drives in a locked drawer/cabinet

Vendor considerations / check list

- Create and disseminate drop sheet style process maps (workflows) accompanied with clear, concise instructions
- Conduct a remote access risk assessment (if not already in place)
- Document remote access per business case including the following information:
    - Justification
    - Employee details
    - Project details
    - Type of content accessed
- Consider time-based access restrictions
- Consider controls to enhance remote access monitoring and associated alerts (e.g., file transfer size limits/restrictions)
- Consider providing 'enhanced' security awareness training to all employees working remotely paying particular attention to phishing emails etc.
- Consider issuing company owned devices for remote access

Vendor assessment evidence/documentation

- Employee NDAs
- Content owner approval

- Workflow maps and associated employee guidelines / instructions
- Network diagrams
- Firewall rulesets and application
- Content transfer policy
- Evidence of any additional security controls implemented (e.g., watermarking)
- Review of Secure Data Destruction policies to encompass home working
- Security awareness training (content and records)

Convergent is providing a remote assessment services for home workers to verify and advise on secure home working based on the above. Our team of assessors in the US, UK and India cover most time zones. We are also providing remote penetration testing in this time of increased cybersecurity risk. We will aim to update this document with further input from our customers.

For more information please contact us:

Mathew Gilliat-Smith UK time zone
mathew.gilliat-smith@convergentrisks.com
Office: +44 (0) 1276 415 725
Cell: +44 771 986 893

Janice Pearson LA time zone
Janice@convergentrisks.com
Office: + 1 818 452 9544
Cell: + 1 323 513 6396

www.convergentrisks.com

Disclaimer: This information is for guidance purposes only and should not be regarded as a substitute for taking technical and legal advice. Document users should seek guidance and clarification from relevant content owners on its adoption and use as applicable. Convergent Risk Inc and Convergent Professional Services Limited exclude any liability arising out of the use of this document.