ACHIEVING WORKFORCE STABILITY

IN A GLOBAL PANDEMIC

Finding a Comfortable Balance with People and Technology

The coronavirus outbreak has demanded unprecedented lifestyle changes. Entire workforces have taken refuge in their homes. For many employees, this might be their first experience working from home. And due to the pandemic's sudden onset, an organization's leadership may not have had the time to communicate work-from-home best practices.

In this guide, we'll offer tips for both employees and employers. Navigating through this crisis where people and technology operate in complementary and synchronous ways. Only by doing so, can organizations continue under a situation with few historical parallels. One goal of this paper is to provide recommendations to help your workers adapt to their new work/life arrangement. Another goal is to ensure their remote employees stay safe, secure, and connected.

> " Working from home isn't a "one size fits all" scenario. Some people, for example, are "segregators" who need to be closed off from personal life (such as in a home office), while others are "integrators" who work better in, say, a kitchen, and with kids and pets around."[1]

Isolated Workers Seeking Equilibrium

When 'social distancing' becomes social isolation, individuals can suffer psychologically. Studies indicate that individuals socially distanced over prolonged periods of time can become depressed, anxious, develop insomnia, and abuse alcohol and drugs. Executives need to know that while their isolated employees appear to be adjusting initially, over weeks and months, the abrupt lifestyle change can take a mental and physical toll.

[1] "Five ways to thrive while working from home during the coronavirus pandemic," by Marc Saltzman, USA Today, March 30, 2020

The loss of face-to-face meetings and the social lunch with co-workers is reviving actual phone conversations. "Verizon says it has seen an average of 800 million wireless calls on recent workdays, nearly twice the volume of Mother's Day."[2]

WORKING FROM HOME A NEW NORMAL

For those employees fortunate enough to work remotely, there are proven practices shared by veterans of the work-from-home experience. Executives need to make sure employees receive tips such as these found in a recent New York Times article.[3]

KEEP THE SAME SCHEDULE

Stick to your schedule as if you were going to the office. "Try to get up at the same time, and do all things you would typically do to get ready for work." Says William Castellano, professor in the Rutgers School of Management and Labor Relations. Also, dress like you would in the office.

SET BOUNDARIES

Pick a spot for your office away from distractions. The same applies for others in the household who are also working remotely. The demands for space and time are even greater as children (and pets) are home and their needs have to be attended to in between work-related tasks.

SCHEDULE BREAKS

Regular meals, exercise, and breaks are as important as scheduled meetings during the day. Losing the pace of a regular day means long stretches of time at the computer, which can be detrimental to physical and mental well-being.

PREPARE FOR ISOLATION

Staying in touch with others becomes crucial to avoid the loneliness of self-isolation. More emails and video and phone calls are not unexpected. For those capable, quiet music in the background can help workers avoid utter silence.

PUT WORK AWAY

Shut down work at the end of the day as if leaving the office. It is especially important during this crisis because "you're already being challenged in terms of your personal resources, you still have to take that recovery time from work," says Dr. Sara Perry, assistant professor of management at Baylor University.

[2] "Call Me Anytime...No Really, We're All Answering the Phone again," by Katherine Bindley, Wall Street Journal, March 26, 2020

[3] "How to Work from Home, if You've Never Done It Before," by Jen A. Miller, The New York Times, March 12, 2020

Technology to Gear Up the Home Office[4]

The work-from-home experience has been made easier in recent years. Accessing an internet connection is now commonplace. The broad use of cloud office suites and SaaS applications offer a seamless experience when transitioning from the office to a home office. But most organizations will not have been forced to support their entire workforce with remote access without much warning or planning. In some cases, sensitive information is confined to access in the office setting, and is not available through remote connection options.

BEST PRACTICES FOR HOME-BOUND EMPLOYEES

People at home tend to be more relaxed about computer security. Their home is their castle. Unfortunately, cybercriminals do not discriminate between office and home office locations, seeking 'soft spots' or vulnerabilities in security. Carefully-engineered phishing exploits and threats can hit home-based workers should they let their guard down.

Check Point researchers surveyed over 400 security professionals since the start of the coronavirus outbreak and discovered these disturbing facts:[5]

- Seventy-one percent of security professionals have noticed an increase in security threats
- Phishing was the leading threat (with 55 percent)
- Malicious websites offering bogus pandemic information (32 percent)
- Malware (28 percent) and ransomware (19 percent) rounded out the results

> “Beware of lookalike domains, spelling errors in emails and websites, and unfamiliar email senders,” Check Point warned. “Ensure you are ordering goods from an authentic source. One way to do this is not to click on promotional links in emails, and instead to Google your desired retailer and to click the link from the Google results page.”[6]

[4] “Practical Tips to Enable Employees to Work Safely from During the Coronavirus Outbreak,” Check Point blog, March 9, 2020

[5] “A Perfect Storm: the Security Challenges of Coronavirus Threats and Mass Remote Working,” Check Point blog, April 7, 2020

[6] “Zoom Domains Targeted by Hackers, as Use Surges with Covid-19,” by Jessica Davis, Health IT Security, March 30, 2020

Here are six steps to fortify your cyber security when working from home:

1. **Passwords matter:** It's a good idea to review and strengthen passwords that you use for logging onto remote resources, such as email or work applications. Do not share passwords with anyone.

2. **Be phishing-aware:** Be wary of clicking on suspicious links and only download content from reliable, verifiable sources. Phishing schemes use social engineering to make an email look real. If the email contains an unusual request, check the sender's details carefully to make sure that you're communicating with colleagues, not criminals. Check Point Research determined that **domains related to Coronavirus are 50% more likely to be malicious**, so casting a cautious and critical eye over every email is important.

3. **Choose your device carefully:** Many employees use their company computer or laptop for personal use, which can create a security risk. The risk is even greater if you use a personal computer for work purposes. If using a personal computer for work, your organization's IT team needs to strengthen its security through mechanisms like strong anti-virus and security packages.

4. **Who's listening in?** Does your home Wi-Fi network have a strong password, or is it open? Make sure it is protected against anyone within range who can possibly access and connect to the network. Unsecured networks make it easier for cybercriminals to access emails and passwords. A LAN (wired) network connection provides even greater security and stability.

   Additional protection tips:

   - If a public instant messaging (What'sApp, Free Teams, Free Slack, etc.) is used, then only non-business information should be shared.
   - With a Microsoft Windows computer, make sure the software is up to date and Microsoft Defender is active. Browsers must also be up to date.
   - With Apple Mac computers, use FileVault for protection.

5. **Video conferencing**: Check Point research has identified the vulnerabilities of video conferencing platforms such as Zoom, Google Classroom, and others.[7] For example, researchers found substantial increases in domain registered names with 'zoom' As many as 4 percent were deemed suspicious. Cyberattackers are taking to 'zoombombing' to join active sessions, spewing hate and vulgarities.
   To avoid this issue, here are tips to secure video conferencing:

   - Always pay attention to those joining a meeting. Ask participants to announce themselves when joining.
   - Ask people to enable video so they can be seen.
   - Apply passwords to meetings, especially where sensitive information is discussed.
   - Prefer the sharing of a specific screen over sharing of your desktop.
   - Do not share a meeting invitation to an unauthorized person or post invitation links on a public website or share them through a personal email account.

[7] "Zoom Domains Targeted by Hackers, as Use Surges with Covid-19," by Jessica Davis, Health IT Security, March 30, 2020

6. **Other remote access tips**

   When connected remotely, do not:

   - Leave a personal computer unattended when connected to the company network.
   - Use the public cloud for sharing business information.
   - Take screenshots.
   - Connect removable devices to the computer.

BEST PRACTICES FOR EMPLOYERS

These pointers serve as a starting point for organizations, whether their apps and data are stored in data centers, public clouds, or within SaaS applications.

- **Trust no-one:** Your entire remote access plan has to be built using the mindset of zero-trust, where everything must be verified and nothing should be assumed. Make sure that you understand who has access to what information — segmenting your users and making sure that you authenticate them with Multi-factor Authentication. Additionally, now is the time to re-educate your teams so that they understand why and how to access information safely and remotely.
- **Every endpoint needs attention:** In a typical scenario you might have people working on desktops/laptops inside the office. Assuming that their devices aren't going home with them, you now have a slew of unknown devices which need access to your corporate data. You have to think ahead about how to handle the threats posed by data leakage, attacks propagating from device into your network, and you need to ensure that the overall security posture of the devices are sufficient.
- **Stress-test your infrastructure:** In order to incorporate secure remote access tools into your workflows, it's critical to have a Virtual Private Network (VPN) or an SDP. This infrastructure must be robust, and should be stress tested to ensure that it can handle a large volume of traffic as your workforce shifts gears from office to home offices.
- **Define your data:** Take the time to identify, specify and label your sensitive data in order to prepare for policies that will make sure that only the appropriate people can access it. Make no assumptions about previous data management and take a granular approach. This will serve you well once remote access is fully enabled. No one wants to accidentally provide the entire organization with access to HR files.
- **Segment your workforce:** Run an audit of your current policies relating to the access and sharing of different types of data. Re-evaluate both corporate policy and your segmentation of the teams within your organization, so that you can appropriately configure access levels, and rest assured that everyone has only what they need.

These cornerstones of remote access security will help organizations better protect their data and networks against threats and interception at both ends of the connection.

Conclusion

The transition for organizations and their employees to shift from formal office locations to home offices requires careful planning and execution. If handled with the aforementioned advice in mind, organizations can take the first step to make the transition smoother and more secure. With the coronavirus testing the resilience of the entire world, the opportunities to learn from one another are immense.

To learn more about Check Point's recommendations for safe and secure remote access computing, visit this page or contact your local Check Point representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com