SANS Institute
Information Security Reading Room

Remote Workers Poll

Heather Mahalik

SANS

A SANS Poll

Remote Workers Poll

Written by **Heather Mahalik**

June 2020

Sponsored by:

ExtraHop

Infoblox

Menlo Security

Pulse Secure

Analyst Program

Executive Summary

The goal of this SANS poll was to see how quickly and effectively we have adapted to working from home in technology-based professions during a time of crisis. On March 11, 2020, the World Health Organization declared COVID-19 to be pandemic—and the "workforce" as we know it immediately changed. Before this pandemic was declared, most of the workforce was not working from home. For example, 68% of respondents reported that less than 30% of their workforce worked from home using computer access to resources. Of these, the majority (47%) reported that this was only 10% of their workforce. The pandemic creates a dramatic swing with 82% of respondents now reporting that 80% or greater of their workforce is now working from home. With the pandemic, the landscape of where people worked drastically changed, as illustrated in Figure 1.

Key topics covered in this paper include how organizations have adapted to:

- Defining organizational roles and geographic distribution
- Adjusting to an immediate need for remote work
- Protecting client and company privacy
- Protecting devices

What percent of your workforce is now working from home using computer access to resources?
Use the date (March 11) when the World Health Organization declared this a pandemic as your reference point.

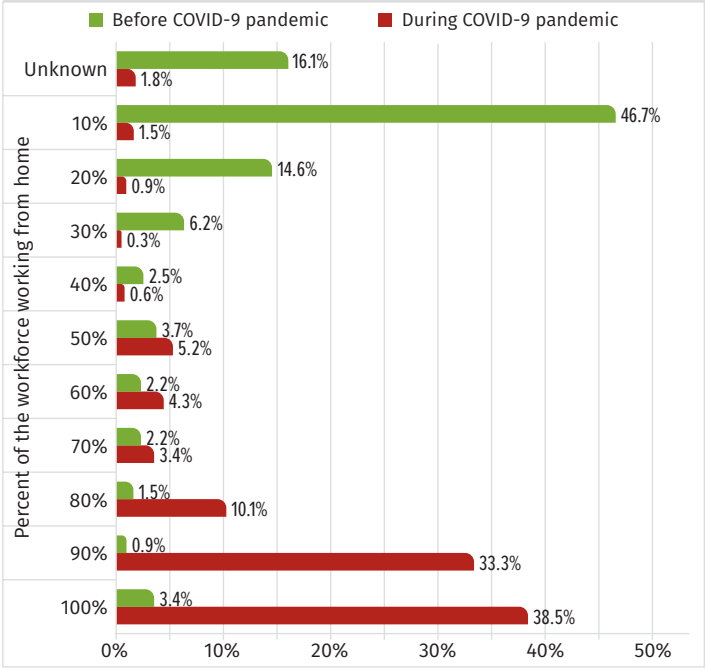

Figure 1. A View of the Workforce Before and After the COVID-19 Pandemic

Remote Workers Respondent Base

The respondents of this survey are in jobs that have traditionally been viewed as office jobs, meaning that workers couldn't do these jobs from home. The respondents include people in jobs ranging from security administrators, IT managers, forensic examiners, pen testers, developers and network administrators to enterprise architects. The ability for people in these roles to rapidly respond and perform their jobs from a new location is nothing less than impressive.

Geographical distribution plays a role in people's ability to adapt to remote work. For example, if everyone the employee works with lives in the same location and/or time zone, it may be easier to work remotely than when team members live across the globe. Consider the employee who hops on a plane every Monday to travel across the country for their work. With travel having decreased for the time being, the majority of people must now work from home. Thirty-two percent of our respondents work in global/multicontinent organizations, 36% are distributed over several states/provinces but remain in a single country, and 24% work solely in a single town/city.

Figure 2 outlines how the respondents' companies are distributed globally.

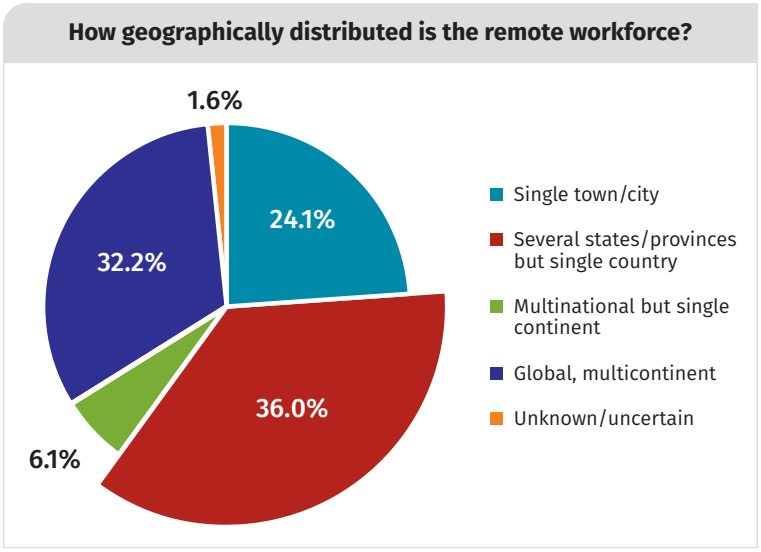

Figure 2. Geographic Distribution of Respondents' Organizations

As you can see in Figure 3, respondents' primary role in their organizations range from C-level executives to administrative assistants.

Takeaway

Your job title, company size and global footprint are not what matters most during this time; what matters is that both small and large companies rallied together to get the workforce running from remote locations.

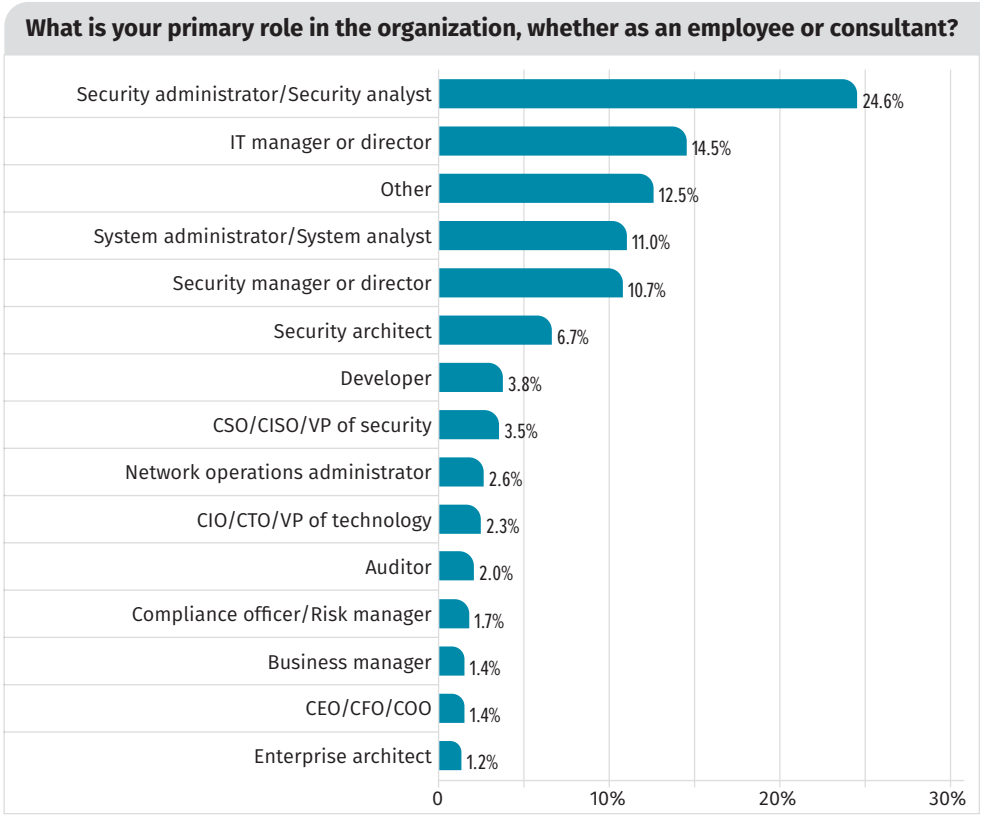

Figure 3. Primary Roles of Respondents

Getting the Job Done

So, how did respondents feel about their organization's ability to efficiently turn on a dime, given the rapid onslaught of the pandemic? How did companies meet their needs during this pandemic with little warning? How did companies protect their data? Was specialized equipment available and accessible? Let's dive in and see how the respondents' organizations stayed afloat and safeguarded their resources.

The Quick Adjustment

Adjusting to remote work isn't easy when you are accustomed to being in an office environment and have certain resources readily available to help you be successful. Figure 4 highlights the resources utilized during remote work.

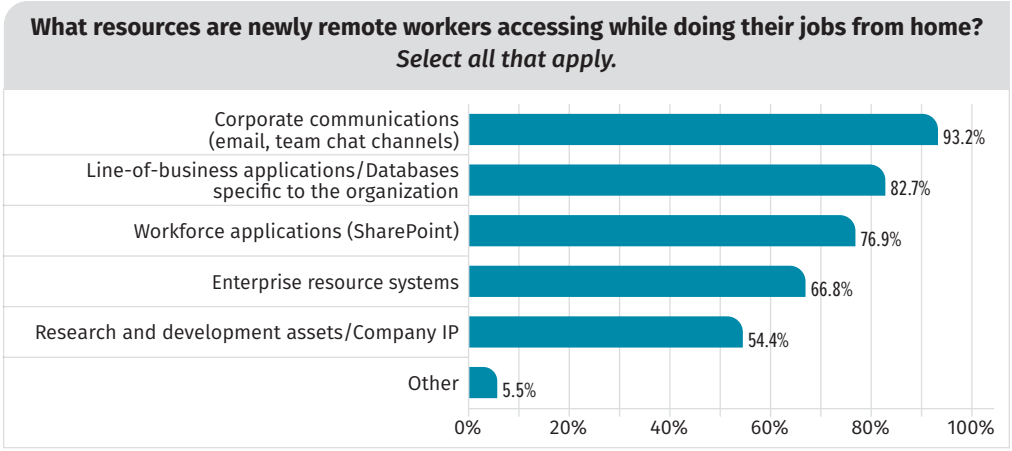

Figure 4. Resources Needed While Working From Home

Takeaway

During the COVID-19 pandemic, we opened doors to different opportunities. We found ways to continue to work from home, we found ways to safeguard our resources, and we proved that working from home can be done even when it wasn't a common practice.

Equipment

Organizations that provide employees with laptops, cellphones and other corporate equipment for at-home use on a regular basis fared a bit better than those that require their employees to leave their equipment at the workplace. Of our respondents, 92% have company-owned laptops they were able to access while working remotely, and a large portion of our respondents relied on both company-owned and personal devices (see Figure 5).

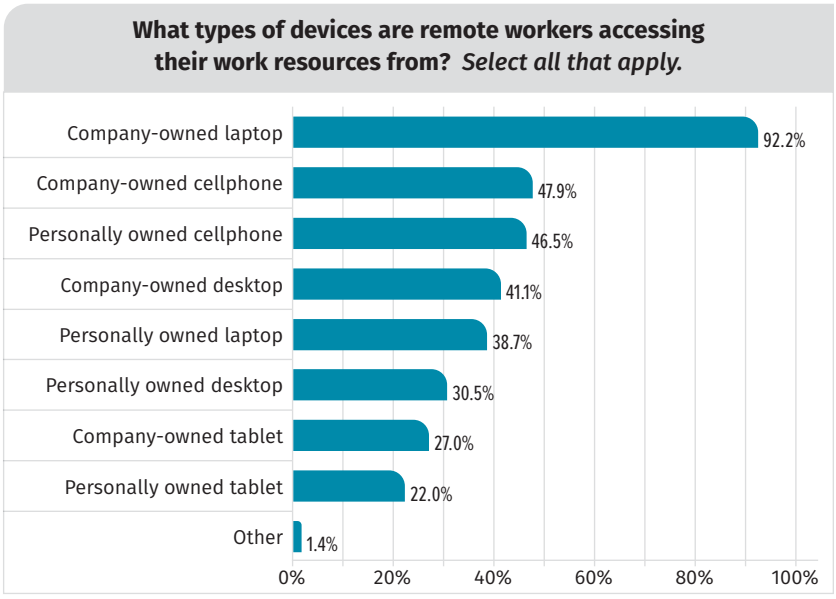

Figure 5. Devices Used for Accessing Work Resources

Action Item

Encourage your company to provide "take home" equipment. This pandemic has shown that unforeseen circumstances happen and oftentimes change our course for completing our work. We need to be prepared and equipped to work no matter where we sit.

Accessing the Data

Having access to data when working remotely is vital to continuing daily operations. As outlined in Figure 6, an astounding 88% of our respondents relied upon VPN and secure connections. Accessing VPN connections is easier if standards of access were in place prior to COVID-19. What if you didn't have VPN access policies in place? What if you didn't have a secure line of communication? HTTPS was the main choice for secure communications, used by 71% of respondents, with others relying on token-based access, Remote Desktop Protocol (RDP), remote sessions, and more.

How are workers accessing their resources? ***Select all that apply.***

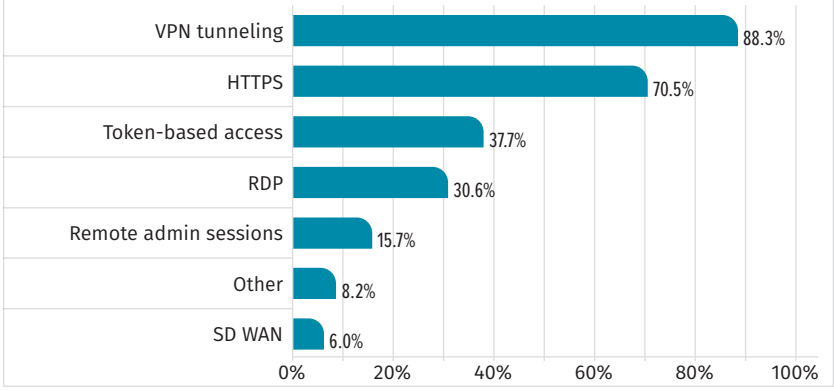

Figure 6. Remote Methods for Accessing Data

Takeaway

VPN tunneling is clearly the most-used method for accessing remote resources. Always being prepared and having this capability in place most likely eased the transition to working remotely.

Focus

Collaboration is key to having a successful team. But how do you accomplish this when you're not sitting in a room together? FaceTime and phone calls add more value than simple email, and it appears that many of our respondents agree. Figure 7 shows that 87% of our respondents conducted voice calls with colleagues. Most used a calling technology that enables collaborators to see one another. Collaboration software such as Google Docs, Trello and Microsoft Teams were used for simultaneous work on the same files. Online conference platforms boomed! Zoom, Webex, Citrix, Skype and others were leveraged by 77% of our respondents. Clearly, we rely upon one another to accomplish our work goals. It's amazing how technology has become a daily tool. This speaks volumes on our choice of career paths in technology and the impact we can have on others.

How do your remote workers collaborate with their teams and share resources? ***Select all that apply.***

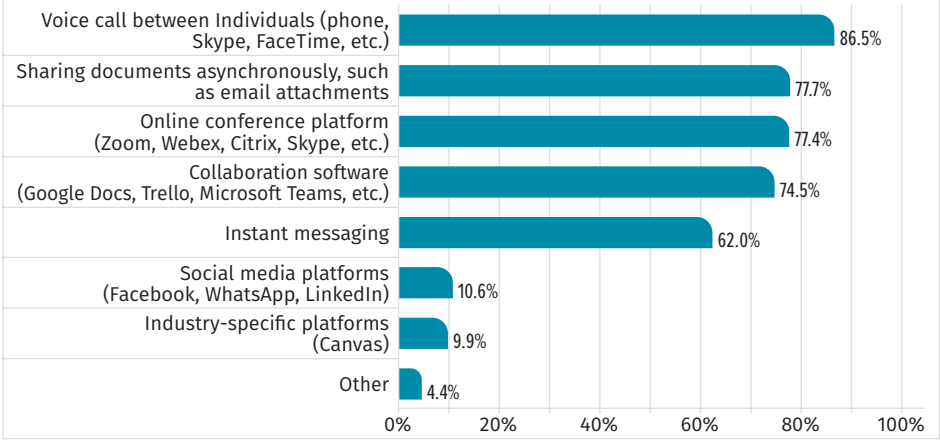

Figure 7. Methods for Remote Collaboration

Action Item

One thing that the COVID-19 pandemic has highlighted is that "face time" with our colleagues matters. Seeing one another when you speak, or simply hearing a voice, goes further than an email or other written modality. Let's keep this going. Let's keep the human aspect and communicate in more human ways.

Protecting the Data

Continuing to protect company, client and employee data is critical as companies rapidly adjust to a new "normal" remote workplace. With this shift, organizations need to determine a way to keep the workflow in action while protecting their assets. While there isn't just one way to protect assets, gaining insights into the ways the respondents safeguarded their work is interesting and can be used as a learning experience for all. Slightly more than 70% of respondents access highly sensitive data about individuals, intellectual property or research (see Figure 8).

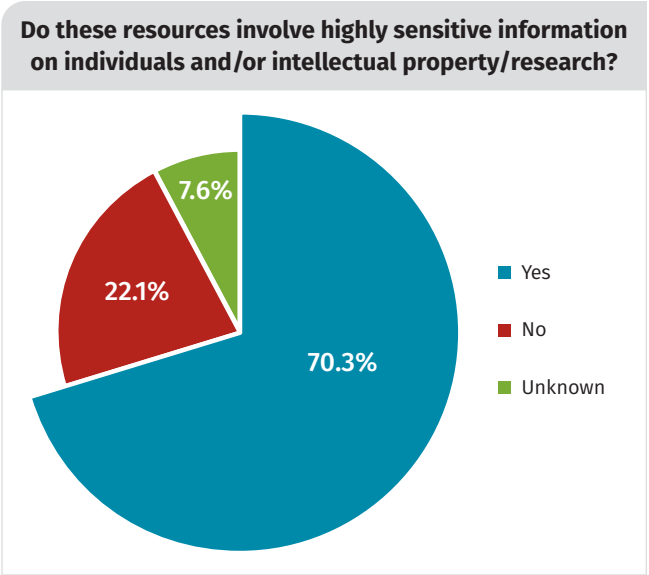

Figure 8. Sensitivity of Company Resources

Corporate resources primarily reside on premises, as shown in Figure 9. This makes sense, given that most of the information remote workers need to access is highly sensitive. Most companies safeguard their assets. The concern is the level or method of access to this sensitive data, which was previously discussed. An interesting aspect of this survey is that almost 56% of respondents rely upon cloud-based platforms, and 40% rely on their internal company private cloud storage. A mere 16% store data in the public cloud. What security mechanisms are in place here to ensure the cloud data is not compromised?

Takeaway

It is of utmost importance for companies to ensure methods of access to sensitive information is secure. Whether considering local or cloud storage, data protection needs to be a priority.

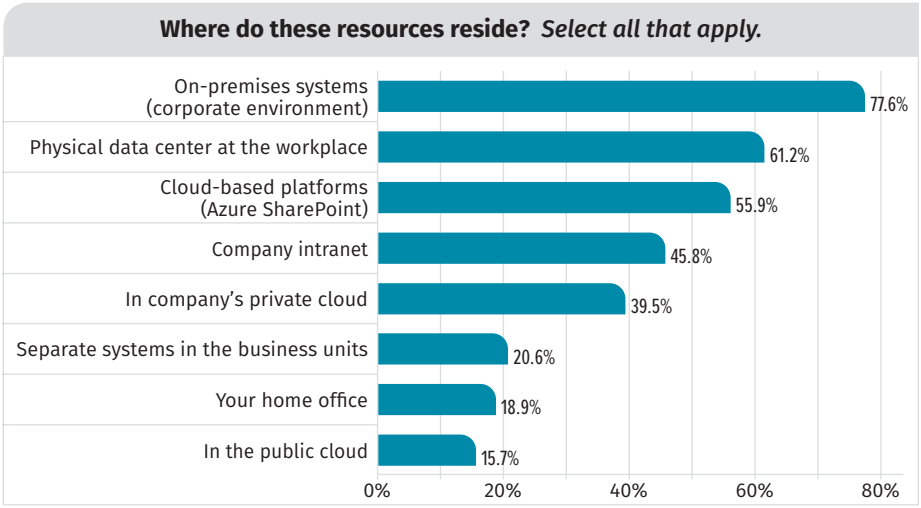

Figure 9. Location of Sensitive Resources

Managing Your Resources

Which devices organizations manage and how they manage those devices varies, as shown in Figure 10. Laptops have the highest rating of being fully managed, while cellphones contain the most managed applications.

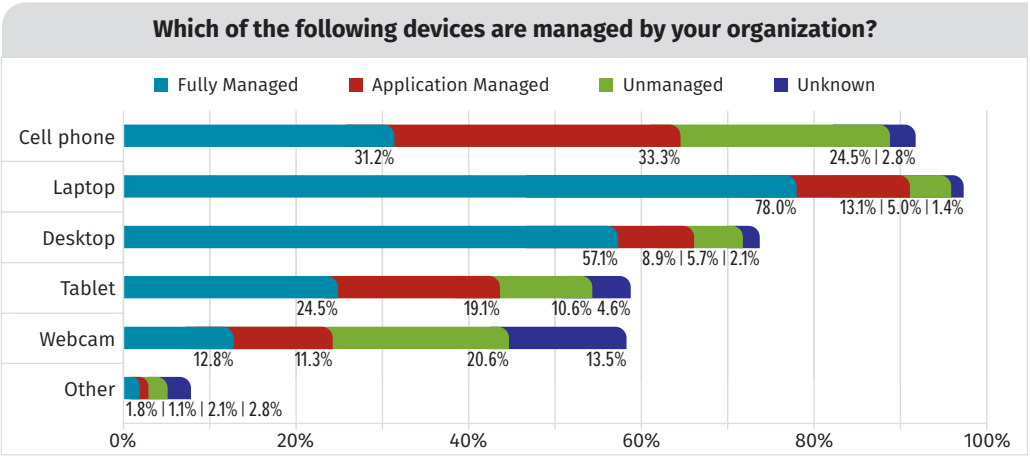

Figure 10. Device Management Statistics

The highest level of security uncertainty appears to be with webcams which, as previously discussed, are heavily relied upon for continuing face-to-face communications.

Action Item

Based on polling results, be wary of hardware protection (i.e., laptop, mobile devices) to protect your privacy while working remotely. Cover up built-in webcams or disconnect external ones when not in use.

Authentication

The next aspect of managing our resources is authentication.

Other authentication methods are also implemented. Almost 42% of the respondents indicate they leverage two-factor authentication, with one form of authentication being a password to access corporate resources. Just over 26% of our respondents are required to use multifactor authentication (MFA), while another 26% simply use a username and password. See Figure 11.

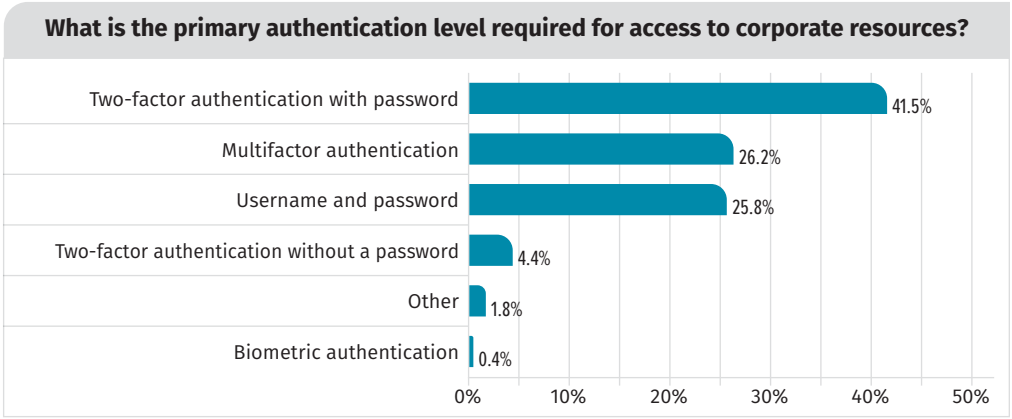

Figure 11. Primary Authentication Levels

Which authentication methods are the best? Are some stronger than others? Does it depend on what you are accessing? These are probably a few of the questions popping up that security teams should discuss.

Action Item

Share this research with your company, discuss the options that work best to protect your resources, develop a plan to implement those options and measure your success.

Conclusion

Organizations were forced to accelerate procedures for remote work during the COVID-19 pandemic. Were they properly prepared? In some cases, yes! This survey shows that most companies reacted quickly and were able to implement traditional workplace security measures in a remote work environment. Implementation plans prior to the pandemic were most likely the reason for success with rapid adaptation and implementation. We need to take this time and reflect on what works and what doesn't.

How did we secure those who were left without work equipment? How did we adjust to global communications and time zone differences? We have all experienced change during this time. Some good and some bad, but one thing is for sure: Technology is needed. Without it, companies would have crashed. We, the techies, have an important role in this world and appear to have selected good career fields.

About the Author

Heather Mahalik is a SANS senior instructor and course lead for FOR585: Smartphone Forensic Analysis In-Depth. As the senior director of digital intelligence at Cellebrite, Heather focuses on forensic research and making the community smarter on all aspects of digital intelligence. Her background in digital forensics and e-discovery covers smartphone, mobile device, Mac and Windows forensics, including acquisition, analysis, advanced exploitation, vulnerability discovery, malware analysis, application reverse-engineering and manual decoding. Prior to joining Cellebrite, Heather focused on mobile device forensics in support of the federal government and served as a technical lead performing forensic examinations for high-profile cases. Heather maintains www.smarterforensics.com, where she blogs and shares presentations.

Sponsors

SANS would like to thank the following sponsors:

ExtraHop
Rise Above the Noise.

Infoblox
NEXT LEVEL NETWORKING

Menlo Security

Pulse Secure®

Last Updated: July 4th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Amsterdam August 2020 Part 1	Amsterdam, NL	Aug 03, 2020 - Aug 08, 2020	Live Event
SANS Reboot - NOVA 2020	Arlington, VAUS	Aug 10, 2020 - Aug 15, 2020	Live Event
SANS FOR508 Canberra August 2020	Canberra, AU	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Amsterdam August 2020 Part 2	Amsterdam, NL	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Virginia Beach 2020	Virginia Beach, VAUS	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS Philippines 2020	Manila, PH	Sep 07, 2020 - Sep 19, 2020	Live Event
SANS London September 2020	London, GB	Sep 07, 2020 - Sep 12, 2020	Live Event
SANS Baltimore Fall 2020	Baltimore, MDUS	Sep 08, 2020 - Sep 13, 2020	Live Event
SANS Munich September 2020	Munich, DE	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Network Security 2020	Las Vegas, NVUS	Sep 20, 2020 - Sep 25, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VAUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS San Antonio Fall 2020	San Antonio, TXUS	Sep 28, 2020 - Oct 03, 2020	Live Event
Oil & Gas Cybersecurity Summit & Training 2020	Houston, TXUS	Oct 02, 2020 - Oct 10, 2020	Live Event
SANS OnDemand	OnlineUS	Anytime	Self Paced
SANS SelfStudy	Books & MP3s OnlyUS	Anytime	Self Paced