WHITEPAPER

Responding to COVID-19

Initial Outlooks and Where We Ended Up

Dropsuite

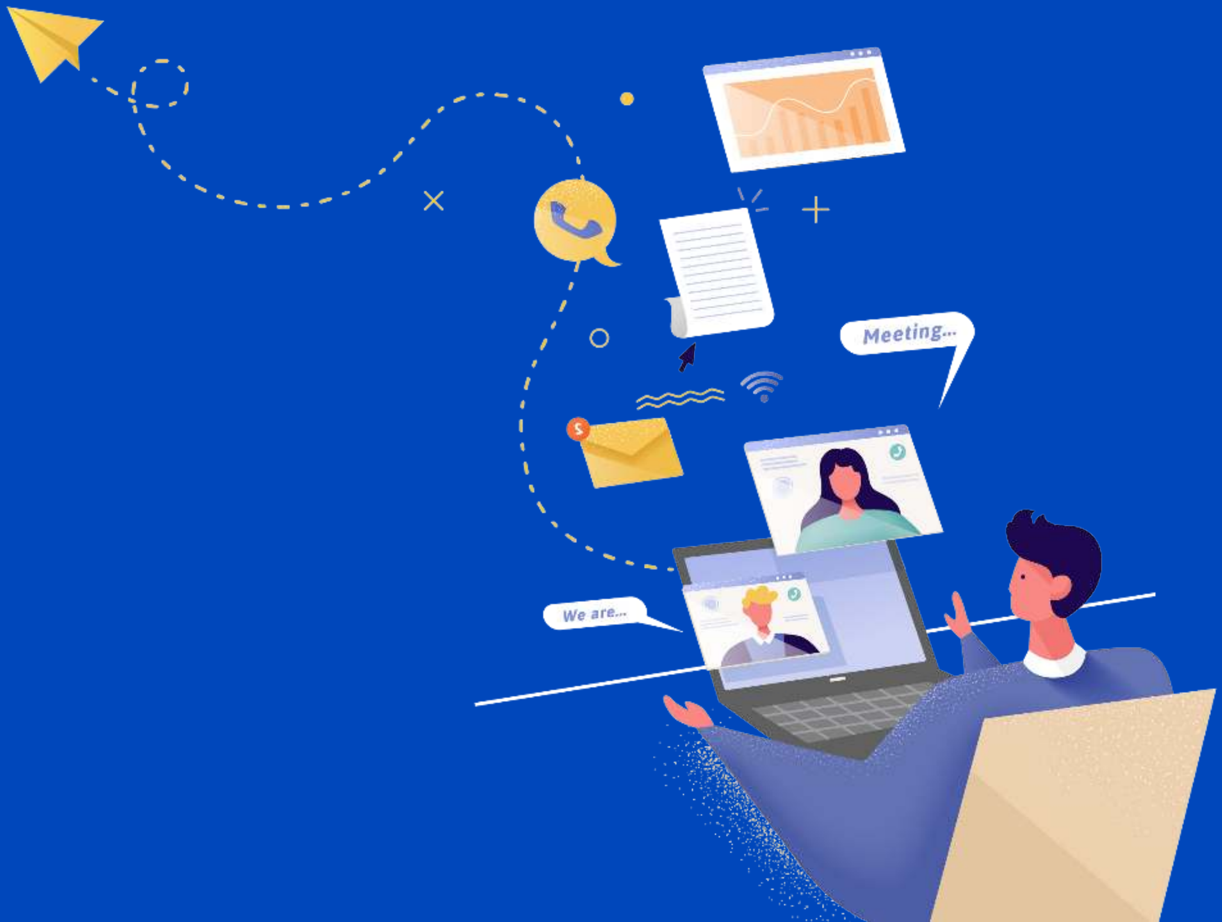
01

Executive Summary

According to the New England Journal of Medicine, the CDC confirmed on January 20th, 2020 that the first US case of novel coronavirus (2019-mCoV), also known as COVID-19, had appeared. Within months, the number of cases had reached over a million people, with potentially millions more at risk. To limit the spread, or “flatten the curve” as it was commonly referred to, the United States and countless other nations began lockdown and quarantine procedures.

Apart from health risks, the primary questions on most people’s minds related to the economic impacts of COVID-19, and the effects that a prolonged lockdown would have on day-to-day productivity. In the early months of 2020, businesses everywhere began a massive transition to how or where work gets done and the technologies that help remote employees stay productive and collaborative.

Towards the beginning of the crisis, Dropsuite commissioned a survey through Osterman Research to see how businesses and industries responded to the shifting work environment, from both a workforce and technology perspective. Months later, we want to examine if those initial trends from Osterman Research’s survey continue to hold true, how they have changed, and what we’ve learned along the way.



02

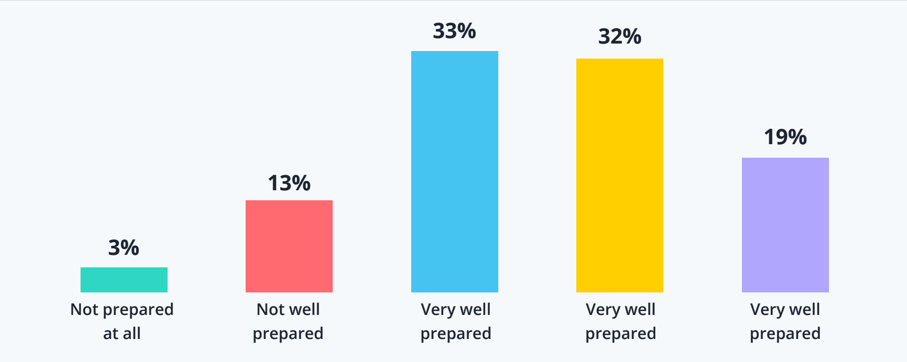
Business preparedness for quarantining and remote work

One of the primary questions asked during the Osterman Research study focused on whether businesses were prepared for the COVID-19 pandemic, and if they could support the shift to remote employees and working from home (WFH).

In general, it appears as if many businesses were not well prepared to deal with the predominant shift to remote work, with less than one in five organizations responding with "very well prepared." It seems that some businesses believed they were adequately prepared, as they had experience with remote employees, but it wasn't until later that they would be able to determine if their preparation could truly scale across their entire workforce for months on end.

Figure 3

Degree of Preparation for the COVID-19 Crisis in Tearms of Having the Technology, Processess and Training in Place to Enable Employees to Continue Working From Home



Source: Osterman Research, Inc.

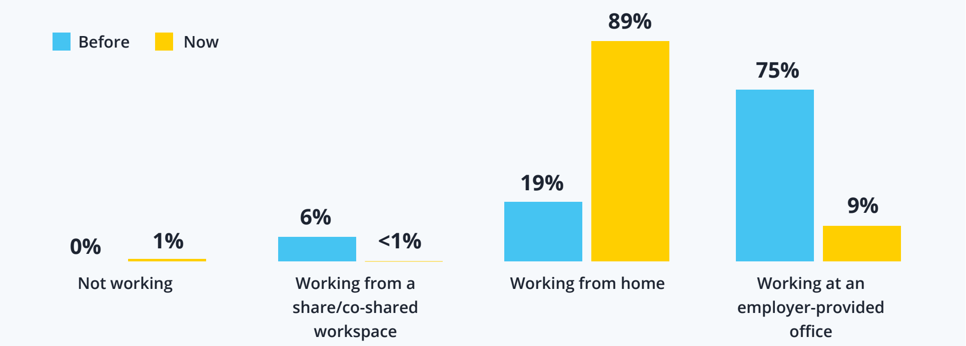
At the time of this survey, in March of 2020, the shift to working remotely was just starting, and not the new normal yet. Many IT leaders believed they had adequately prepared for the transition when it came to technologies that enable remote work. Initially, preparedness looked like business continuity planning, adopting the right technology solutions, and having the appropriate resources available for employee distribution. For most, this translated to utilizing Cloud technologies for hosting critical data and applications, using remote productivity solutions such as Microsoft 365 (Office 365) or Google G Suite, or being able to provide laptops for employees to take home. In such cases, businesses leveraging these technologies thought they were prepared for a smoother transition than most, but even with those technologies having already been adopted, there were other challenges that hadn't been considered at the beginning of the COVID-19 pandemic.

03

Employee preparedness in the shift towards remote work

With lockdown mandates coming from Government and Medical leadership, the simplest response was for people to start working remotely, and from home. The Osterman Research survey shows, this lockdown resulted in a significant increase in remote workers, the scale of which was unprecedented.

Figure 1
Work Status of Survey Respondents Before and During the Current Crisis



Source: Osterman Research, Inc.

Prior to COVID-19, one in five employees had a remote job. After the onset of COVID-19, that number jumped dramatically to four in five jobs being remote. With such substantial and sudden increases in the number of remote workers, businesses saw varying degrees of preparation among employees, depending on the technology they had already adopted. Businesses already using technologies such as SaaS-based (Software as a Service) productivity suites didn't have too much trouble making the transition, as employees were already familiar with those tools. However, for many, these tools had to be quickly adopted, and employees had to be quickly trained. Basic best practices such as saving all work files to OneDrive or Google Drive, or techniques on sharing large files that can't be attached to emails, were suddenly a daily challenge that needed to be addressed in short order.

Figure 4

Current Practices Resukting From the COVID-19 Crisis

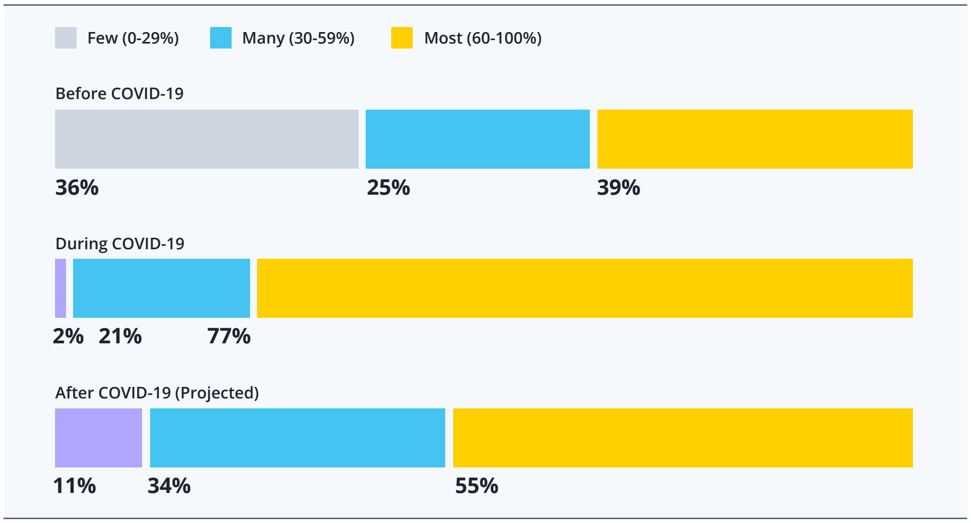
Issue	%
Our IT team has seen an increase in helpdesk calls because many employees are new to working from home	67%
We are permitting employees to use their own device (e.g., desktop, laptops, smartphones, etc.) when working from home	52%

Source: Osterman Research, Inc.

Some of the key problems that employees encountered revolved around access to company-owned devices, resulting in personal devices being used for work. In addition, many employees found themselves reaching out to IT Helpdesk Support resources to deal with the new issues resulting from remote work. These issues created an initial wave during the transition to remote working and have likely leveled off. However, businesses should be prepared to deal with potential future increases, as some issues can impact multiple people all at once. Preparing an IT helpdesk infrastructure to deal with spikes and address multiple users at once can help mitigate common challenges experienced by a remote workforce.

According to PwC, 72% of office workers would like to work remotely at least two days a week, with high support for flexible working in general.

What percent of your office employees do you anticipate will work remotely at least one day a week?



Source: PwC US Remote Work Survey. June 25 2020. Base: 120 US executives

Recent PwC surveys project that at least 50% of employees anticipate working from home at least once during the week, meaning that working remotely is no longer a temporary solution, but rather a long-term reality. IT organizations that have made adjustments and learned to adequately support a majority remote workforce will be able to accommodate any level of WFH company policies going forward. As some offices reopen and employees return to the office, IT will likely be well prepared to serve employees regardless of their location.

04

The Long-Term Implications of Working from Home

Dedicated workspaces in the home

Once the business world came to terms with remote working being the new normal, many business leaders not only reexamined business and employee preparedness in key areas but also understood there were long-term implications that were initially unforeseen, such as adequate home office spaces, video and audio considerations, as well as networking and security best practices.

Having a dedicated working environment at home became critical, but many employees had to make do with wherever they could fit a laptop. Too many workers found themselves working around the house, whether it was the kitchen, living room, or any other area with a flat surface. It seemed as if most remote workers were unprepared or lacked the space to establish a home office with adequate equipment. Organizations can help their employees stay comfortable while working by providing guidance and equipment. Ergonomic desks, chairs, and other computer peripherals help ensure employees don’t get fatigued by working in uncomfortable positions for long hours. Employers should prioritize employee mental health and work towards ensuring employees are well-equipped at home to continue working in a healthy and ergonomic way.

With virtual meetings becoming a primary vehicle for live collaboration and interaction, many remote employees found themselves with sub-par video and audio capabilities, making it difficult for virtual meetings on Zoom or Teams. Whether it was camera placement, microphone quality, lighting, or environmental noise, many workers experienced difficult virtual calls with poor quality and too many distractions. Employees have seemingly worked these challenges out on their own, but guidance from business leaders may have reduced some of the friction.

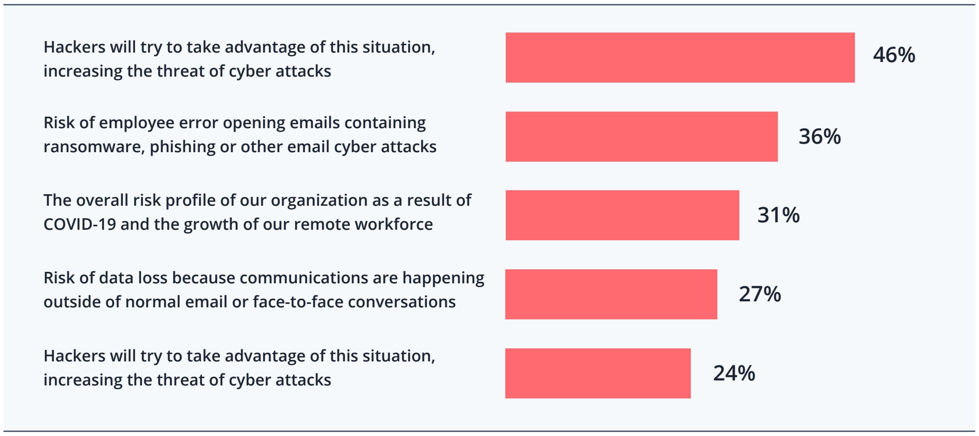
The cybersecurity and data protection question

Cybersecurity professionals have seen a dramatic increase in cyberattacks looking to leverage the COVID-19 chaos for nefarious purposes. As a result, many IT and security professionals realized data protection solutions and security training were areas where early investments would have helped immensely due to new and increased risks regarding remote work.

Figure 7

Concerns About Various Issues

Percentage responding “Concerned” or “extremely concerned”



Source: Osterman Research, Inc.

COVID-19 has presented huge risks and opportunities for potential bad actors and hackers to leverage for cyberattack vectors. IT Security and Compliance Teams initially had to scramble to support their now-remote workforces. As many employees are likely using potentially unsecured home networks and increased use of personal devices, IT Security teams found themselves in an unprecedented situation. To overcome these new challenges, many IT Security teams sought to deploy new security protections such as multi-factor authentication, VPNs, and password requirements to bolster security and eliminate unauthorized access to critical systems and data.

Increased email usage may result in phishing or other email cyberattacks slipping through, as well as ransomware attacks through new vectors such as remote workers. Targeted email attacks such as spearphishing can be especially dangerous with everyone working remotely. If an employee gets a malicious email from someone posing as company leadership, it can be difficult to verify authenticity without simply verifying in-person. In addition, malicious links and other email-based cyberattacks can create tremendous vulnerability for a company and its critical data.

Bad actors are leveraging the ongoing pandemic to fuel fears and urgency by registering domains meant to emulate CDC, medical, or Government websites to gain information. These types of cyberattacks are often sent through emails and lead to an organization's systems becoming compromised. It is critical to educate employees on how to identify such attacks, and what they can do to avoid becoming a vector for security being compromised.

Organizations should also strongly consider additional email security solutions as well as data backup procedures to ensure critical business data is always accessible. Working remotely means device-stored data is also remote, which necessitates a robust backup solution to ensure employee data remains accessible and recoverable in cases of emergency.

In the long term, IT Security and business leaders should strongly consider working closely with employees to determine at-home network security readiness and consider making investments to bolster remote employee security. Issuing security hardware such as routers or firewalls may be necessary for employees who work closely with critical data. Such solutions, in addition to improving network connectivity, may be necessary for certain employees. Each worker will need to have their home network capabilities assessed on an individual basis to best determine priority for more specialized security needs.

COVID-19's Impact on Network Utilization

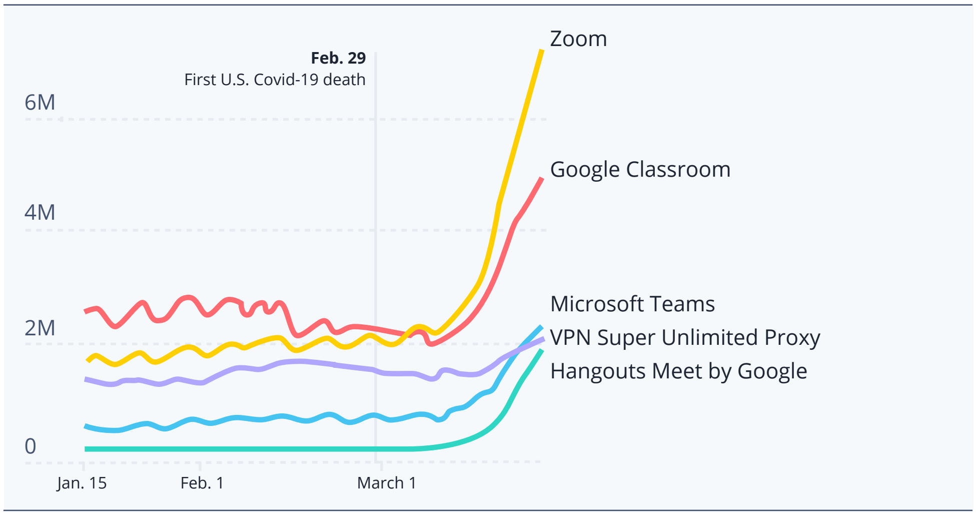
Businesses often pay a premium for high-bandwidth connectivity in their office spaces. When work needs to be done in a timely manner, a slow network becomes a major bottleneck to corporate and employee success. With everyone now working remotely, the home network has become the business network. Each employee likely has internet connectivity, but depending on the services they utilize, they may have limitations regarding speed and bandwidth, which can negatively impact their ability to perform work.

> With everyone now working remotely, the home network has become the business network.

Whether it is virtual meetings, video streaming, or transferring large documents, Internet Service Providers (ISPs) have seen a dramatic increase in network utilization across the board. For example, the New York Times saw dramatic increases in remote work app usage across professional, educational, and private usage.

We have suddenly become reliant on services that allow us to work and learn from home

Daily app sessions for popular remote work apps



Source: Osterman Research, Inc.

In addition, Microsoft reported in late April that Microsoft Teams usage dramatically increased 70% to over 75 Million daily active users, with 200 million meeting participants in a single day. Microsoft CEO, Satya Nadella even highlighted that two-thirds of Teams users are sharing files and collaborating, and that Microsoft has seen triple the number of organizations integrating apps with Microsoft Teams.

Remote work has altered how home networks are being utilized. Similar to the cybersecurity concerns highlighted previously, it may be necessary for IT Support teams to work with employees to determine if network upgrades are needed. It is also critical to create a dialogue around balancing employee privacy at home and the need for robust business security. Employees should be made aware of what is within the purview of IT Security, and how to avoid conducting personal activity in a way that is visible to their employer's IT teams. Employees may want to utilize separate work and home devices, VPNs for business network activity, or other solutions that help compartmentalize work and personal activity.

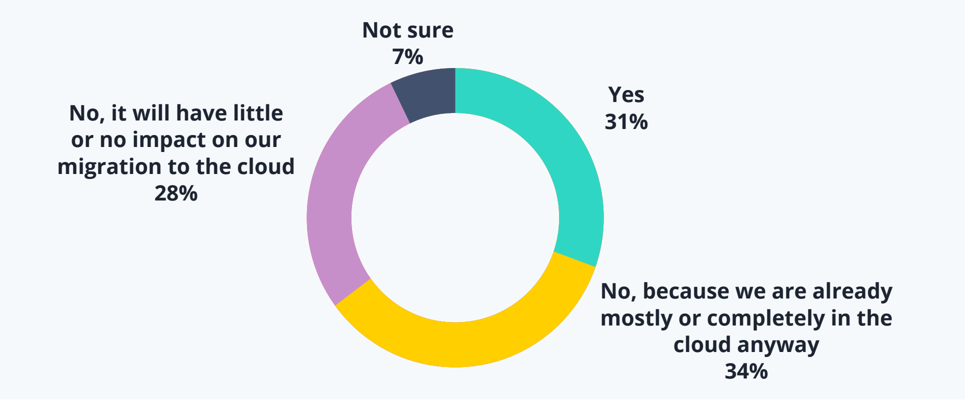
In addition, existing employee home networks may simply lack the network data bandwidth needed for certain types of work. In such cases, employers should determine if it's possible to upgrade network hardware such as routers, or if worker's internet services from ISPs should be upgraded to a higher tier of service.

Long-term investments in IT Infrastructure

When it comes to major IT infrastructure considerations, businesses have been seeking out a new IT infrastructure for data, applications, and services, leading many to believe that the Cloud has the ideal solutions.

Figure 17

"Will the current situation accelerate your oganization's migration to the cloud?"



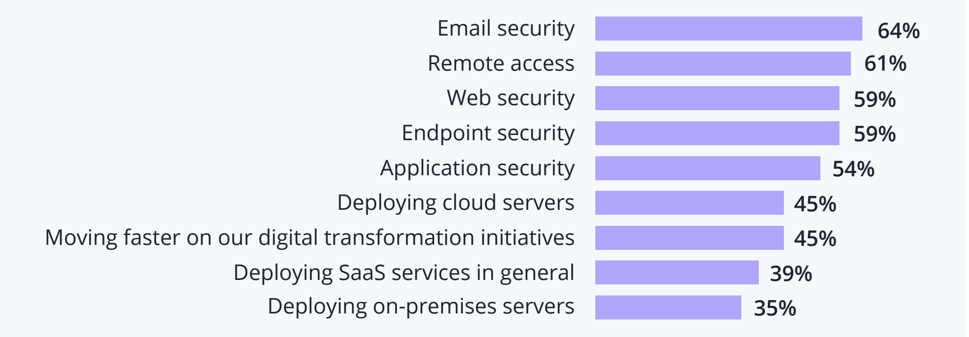
Source: Osterman Research, Inc.

With nearly half of respondents who are not yet using the cloud indicating they will increase cloud adoption, it is clear that COVID-19 has led some organizations to see the cloud as a solution to many challenges regarding IT infrastructure. In an increasingly decentralized working environment, the cloud can be leveraged as a key component for centralized IT infrastructure and services, a single solution that provides the IT backbone for businesses whose employees are now geographically scattered.

Figure 20

Priority for Augmenting Various Corporate Capabilities

Percentage responding a "high" or "very high" Priority



Source: Osterman Research, Inc.

This increase in cloud adoption may translate to leveraging IaaS (Infrastructure as a Service) solutions such as data storage, SaaS (Software as a Service) solutions such as Microsoft 365 and Google G Suite, and PaaS (Platform as a Service) for development frameworks or analytics. Each level of cloud usage offers tremendous benefits for businesses looking to move away from on-premises data centers.

In addition to businesses accelerating their migration to the cloud, the COVID-19 pandemic has triggered a reordering of priorities for many IT organizations. Most respondents highlight priority around security and remote access capabilities. However, the primary concern focuses on email security. Email has become the primary method of communication outside of virtual calls, and as a result, employee inboxes are likely to be busier than ever before.

Unique industries have unique needs

Certain industries have found themselves completely reimagining how they get work done. Healthcare has seen a dramatic increase in "telehealth" services where patients connect via virtual meeting spaces to discuss health needs and even triage, screen, and diagnose patients. Cloud providers such as Microsoft have recognized these specialty needs and introduced new capabilities since the COVID-19 pandemic started, such as Azure for health. As hospitals continue to see new COVID-19 patients, many healthcare seekers are wary of potentially exposing themselves via physical visits to the hospital. This will likely continue even as new COVID-19 cases reduce in the future, so new cloud-based healthcare services and infrastructure are likely to remain for the foreseeable future.

Industries like Healthcare and education have had to entirely reimagine how tey get work done in this new COVID environment.

Education has seen a dramatic shift towards online learning following mandated lockdown orders. It is clear that the Education sector was largely unprepared for this shift towards online learning and the challenges of supporting a remote student body. School IT teams had to quickly adjust their networking security best practices to allow external connections from student's homes while also ensuring cyberthreats were adequately defended against. Both Microsoft and Google offer education-specific cloud services with the goal of providing learning materials, quizzes/testing, virtual classrooms, and other tools for students, educators, and educational institutions. Many governments are hesitating to reopen schools, which means such cloud services will likely continue to see higher rates of adoption. These services are likely to change over time as schools begin to reopen, but they make for a capable foundational infrastructure whose value became readily apparent during the COVID-19 pandemic.

Other industries have undergone similar changes and are likely to continue down the path towards cloud adoption as such services offer scalability and universal access in a way that on-premises solutions could not provide.

05

What we’ve learned, and what it means for the next potential global crisis

COVID-19 and its global impact have forced us to reimagine what “disaster recovery” truly means in the technology space. Until COVID-19, most experts considered and prepared for natural disasters and events that could physically affect the infrastructure of critical data systems. “Disaster recovery” often focused on computing hardware systems becoming compromised, but COVID-19 forced many organizations to understand that disaster recovery now includes risks around the humans who manage such systems as well.

COVID-19 has rescoped what a “disaster” could mean, and what business continuity planning truly entails in the modern era. Ultimately, flexibility is a key determining factor as circumstances change very quickly, and businesses must be able to respond equally fast. Transitioning to near-full remote work in mere weeks highlighted the value of investing in Cloud-based solutions. Being able to leverage a global managed infrastructure for critical data systems not only limited employee exposure to potential risks, but it made the transition to remote work much easier. Employee familiarity eased IT Helpdesk bandwidth and seemingly prepared many for virtual meetings and collaboration. Employee knowledge of best practices for file sharing, backups, and using shared drives helped with file management and collaboration.

Looking forward, it should be assumed that remote work is going to become much more common. Employees have come to appreciate the flexibility of working from home and have come to expect a similar level of flexibility to be offered by their employers. Businesses should invest in technology solutions, training, and resources that help ensure employees can do the best work they can, regardless of their physical location. Companies should seriously consider investments into cloud infrastructure services, and other services that offer a decentralized distribution across their workforce, such as security-oriented SaaS solutions. Businesses onboarding new employees should train their workers as remote-first, as those skills will easily translate to the physical office.

Looking forward:

- Invest in technology solutions, training, and resources
- Consider investments into cloud infrastructure services
- Train workers and new employees as remote-first
- Ensure data is accessible, backed up, and following critical regulatory requirements

A critical area for businesses and IT teams to consider is how to consolidate data, documents, and communication that is now spread across employee devices. Ensuring data is accessible, backed up, and following critical regulatory requirements should be considered a major priority. Despite the dramatic shifts various industries have experienced as a result of COVID-19, there is little leeway when it comes to following data protection regulations. Investing in the right solutions early on and establishing a foundation of such data backup solutions into your infrastructure can eliminate many issues resulting from situations like a global pandemic.

06

Guidance and consideration for security and data protection

The COVID-19 pandemic has reframed what business continuity truly means, and for many organizations, IT Teams were unprepared for dealing with this new reality. Some key considerations are:

- Do employees have appropriate physical workspaces at home?
- Do employees have access to appropriate devices, network connections, and security capabilities in their new makeshift home offices?
- Are employees at greater risk of falling victim to social engineering attempts such as phishing attacks?

To proactively deal with these considerations, organizations can provide access to the right tools and solutions such as:

- Guidance regarding ergonomic desks, chairs, and other equipment to ensure employees can work comfortably.
- Purchasing new devices, whether it is laptops, routers, or other critical hardware to maximize performance, bandwidth, and security.
- Authenticating corporate-sponsored identity such as hardware security keys or multi-factor authentication.
- End-to-end encrypting of critical communication and data systems.
- External access controls for corporate communication platforms such as virtual meeting spaces or file-sharing apps.
- Monitoring tools to monitor employee activities and experiences for both compliance and proactive IT Help Desk capabilities.
- Tracking data routing or processing locations in order to follow geography-based regulations such as Europe’s GDPR.
- Adhering to critical data protection standards for specific industries or market sectors such as healthcare, financial services, or education.
- Integrating backup and archiving tools to ensure all essential records and data are captured, secure, and accessible at all times.

07

How can you prepare for the future?

While there are a number of solutions that provide organizations with a centralized collaboration platform, we believe the best options are Microsoft 365 / Office 365 and Google G Suite. Both SaaS productivity solutions provide cloud-based document storage, messaging and communication tools, as well as security-enabled management tools. While both platforms enable business continuity and provide remote workers with powerful capabilities, neither have adequate backup and archiving capabilities for documents, data, and communications.

Dropsuite solutions for Microsoft 365 / Office 365 and Google G Suite provide customers with the tools to ensure their critical documents, emails, and data are backed up, GDPR, HIPAA, and FINRA compliant, as well as protected by military-grade 256-bit AES encryption. Dropsuite not only backs up your emails, documents, cloud storage, and chat communications, but provides such services at an affordable cost, and with easy deployment. Dropsuite is here to help reinforce your business continuity plans, which is a key priority in today's unpredictable world.

Learn more about Solutions:
Telephone: NA Sales: **+1-408-780-2106**
Telephone: Int. Sales: **+65 6813 2090**
Email: **sales@dropsuite.com**

About Dropsuite

Dropsuite is a cloud software platform enabling businesses and organizations globally to easily backup, recover and protect their important business information. Dropsuite's commitment to advanced, secure, and scalable cloud technologies keeps us in the forefront of the industry and makes us the choice of leading IT Administrators and Service Providers globally.

Dropsuite