Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **April 2020**
Sponsored by **Zix**

Was Your Company Ready for COVID-19 and Is It Prepared for Future Emergencies?

Executive Summary

The COVID-19 pandemic has had profound and unprecedented impacts on a global scale. The most common response of governments to the pandemic has been to implement "social distancing", "stay-at-home", "shelter-in-place" or similar types of edicts, which have forced millions of businesses to shut down their normal operations. Those that can continue operating have been suddenly forced into a situation in which employees and contractors are now working from home or other remote locations for an indeterminate period, causing IT, security, compliance and other staffers to scramble to accommodate a very different workplace paradigm.

To understand the impact of governmental requirements to shut down normal business operations, Osterman Research conducted an in-depth survey of more than 400 IT decision makers and influencers, primarily in the United States. This report presents the results of that research and offers best practice guidance around what decision makers may want to consider as they navigate the current crisis and plan for future eventualities. It's important to note that while the topic of this paper relates to the current pandemic, the advice offered herein will be useful to decision makers and influencers who must plan for future crises, whether limited in scope to a particular region after an earthquake or hurricane, for example, or to another global event.

KEY TAKEAWAYS

Here are the key takeaways from the research:

- Before the COVID-19 crisis, 18 percent of employees in the organizations surveyed were working from home; today, that figure is 80 percent. What makes this a very difficult and risky proposition for many organizations is that only 19 percent of IT decision makers and influencers believe their organizations were "very well prepared" to deal with a crisis like this before it began.

- Underscoring the point above, 70 percent of organizations report that the current crisis has negatively impacted their ability to maintain normal operations. However, 17 reported that the crisis has had almost no impact and, somewhat surprisingly 14 percent report it has actually improved their operating situation.

- Decision makers are relatively pleased with their employees' ability to continue communicating with employees and others via the corporate email system: 81 percent reported that this aspect of their communications is going "well" or "very well". Similarly, 71 percent report that employees' ability to replace in-person meetings with video meetings is also going "well" or "very well".

- Conversely, activities like employees sharing files with others and employees having access to the equipment and technology that they need to do their work is being met with difficulty: fewer than two-thirds of organizations report that these issues are going "well" or "very well".

- There are a number of concerns that IT decision makers and influencers have about the current work-from-home phenomenon: 46 percent are concerned that hackers will try to take advantage of the current situation of employees suddenly working from home, thereby increasing the threat of cyber attacks. Thirty-six percent are concerned about the risk of employees erroneously opening emails that contain ransomware, phishing or other email cyber attacks.

- Not surprisingly, video/meeting technologies have seen a significant increase in use by work-from-home employees relative to their use before the crisis began: use of Zoom has gone from 31 percent of users before the crisis to 48 percent now; WebEx has seen an increase from 39 percent to 42 percent. Microsoft has seen an enormous increase in the use of Teams – from 32 million to 44 million

There are a number of concerns that IT decision makers and influencers have about the current work-from-home phenomenon.

users in a week's time[1] – particularly in areas first hit with the virus in various locations in Europe. Other technologies, however, have largely stayed flat or have seen a small decrease in use.

- Compliance and continuity look to be trouble spots for many organizations in the near future. For example, only 72 percent of organizations are backing up all of their data as they were before the crisis, and only 59 percent are archiving all of their data as they were before.

- Will the current situation accelerate organizations' migration to the cloud? In many cases it will: 30 percent reported that the crisis will accelerate their migration, while another 34 percent reported it will not, but only because their organization is mostly or completely in the cloud already. Only 28 percent reported that the crisis will not have much of an impact on their cloud migration initiatives.

- One long-term result of the current crisis may be that many more employees will be working from home. Once the crisis has passed, 10 percent of organizations report that they will want the majority of their employees to remain remote, 18 percent plan to implement a new work-from-home policy for employees to work at least partially from home, and 27 percent will want employees to remain remote. Only 44 percent will want everyone back in the office or as they were working before.

- This crisis is prompting many IT decision makers and influencers to augment many of their current capabilities. For example, 64 percent of organizations are placing a "high" or "very high" priority on bolstering email security, 61 percent give this high a priority to improving remote access, and 59 percent give this high a priority to improving both web and endpoint security.

One long-term result of the current crisis may be that many more employees will be working from home.

ABOUT THE SURVEY AND WHITE PAPER

The survey conducted for this white paper was conducted from April 6-9, 2020.

This program was sponsored by Zix; information about the company is provided at the end of this paper.

Survey Results

This section includes the full results from the survey.

RESPONDENT DEMOGRAPHICS

A total of 404 surveys were completed with IT decision makers and influencers, mostly in North America. Here are the details on the organizations that were surveyed:

- The mean number of employees at the organizations surveyed was 12,980; the mean number of email users was 12,526.

- Surveys were conducted in the following countries:

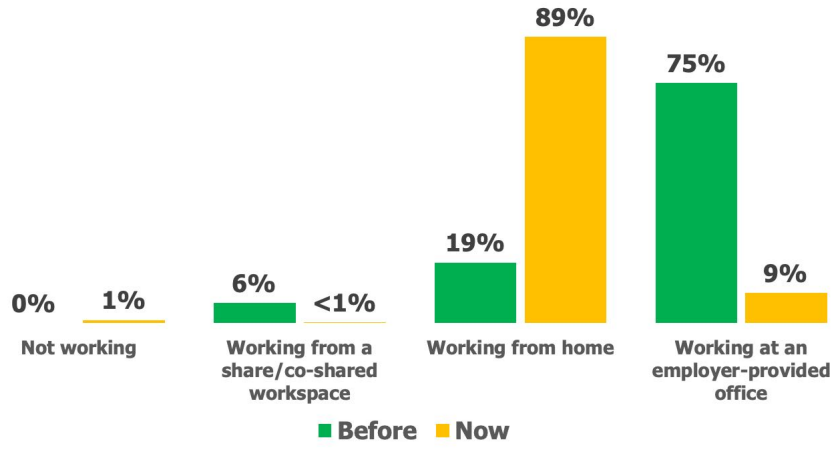
    - United States: 97.3 percent of surveys conducted
    - Canada: 1.2 percent
    - United Kingdom: 0.5 percent
    - Unspecified: 0.4 percent
    - Spain, Brazil and Germany: 0.2 percent each

[1] https://www.theverge.com/2020/3/19/21186452/microsoft-teams-new-features-noise-supression-user-increase-coronavirus

- The top five US states in which the survey respondents work are:
    - California: 14.2 percent of US-based respondents
    - New York: 11.2 percent
    - Texas: 7.1 percent
    - Florida: 5.9 percent
    - Illinois: 5.6 percent
    - Thirty-nine other states: 56 percent

The work status of the individuals who completed the survey is shown in Figure 1.

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



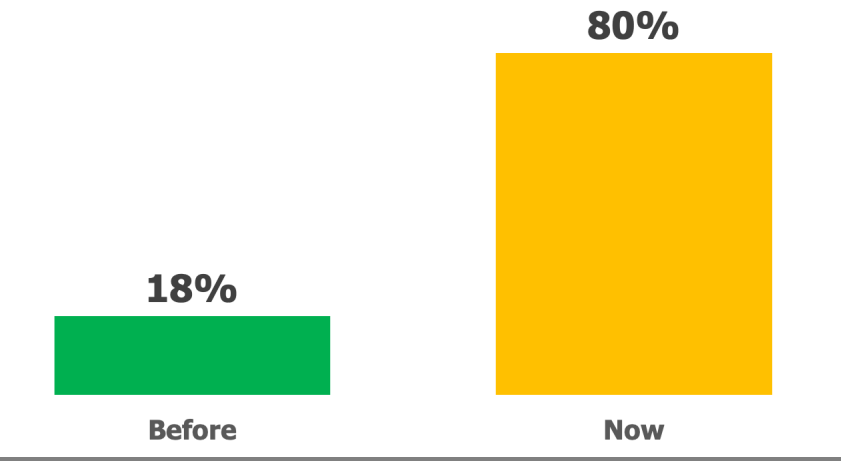
Source: Osterman Research, Inc.

A HUGE INCREASE IN EMPLOYEES WORKING FROM HOME

We discovered that there has been a rapid increase in the number of employees working from home as a result of the COVID-19 crisis. As shown in Figure 2, just under one in five employees had a work-from-home job prior to the COVID-19 crisis, but that number has jumped dramatically to four in five.

...under one in five employees had a work-from-home job prior to the COVID-19 crisis, but that number has jumped dramatically to four in five.

Figure 2
Proportion of Workforce Working From Home Before and During the COVID-19 Crisis

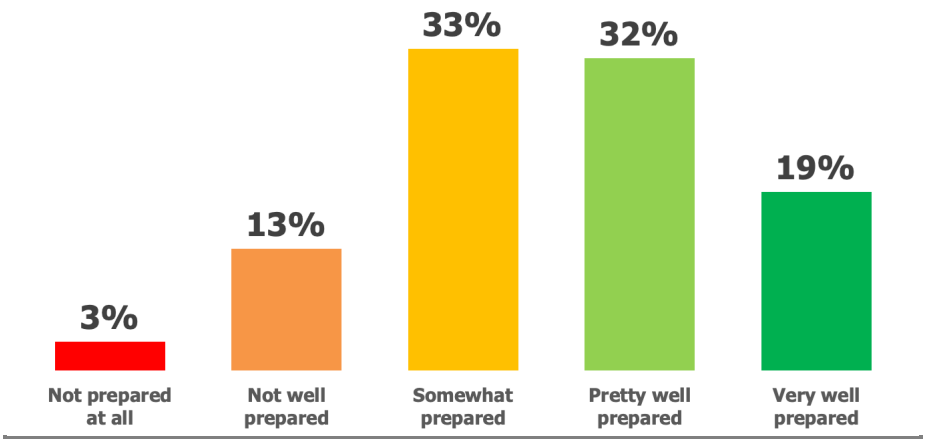


Source: Osterman Research, Inc.

MOST WERE NOT WELL PREPARED

Fewer than one in five organizations were "very well prepared" for the COVID-19 crisis in the context of having their employees and contractors suddenly forced to work from home, as shown in Figure 3. Moreover, another 32 percent felt they were "pretty well prepared" to deal with the sudden work-from-home phenomenon.

Figure 3
Degree of Preparation for the COVID-19 Crisis in Terms of Having the Technology, Processes and Training in Place to Enable Employees to Continue Working From Home



Source: Osterman Research, Inc.

In hindsight, IT decision makers should have been prepared for this type of crisis in the context of business continuity planning, having the appropriate resources available to distribute to employees, having their employees trained properly, deploying the right security and data protection solutions, and so forth. But when budgets are tight and IT and security decision makers are in regular firefighting mode, it's not difficult to see why many organizations simply don't have the strategic foresight and financial bandwidth to accommodate capabilities to deal with extraordinary events like this one.

Fewer than one in five organizations were "very well prepared" for the COVID-19 crisis.

PROBLEMS WITH THE SUDDEN WORK-FROM-HOME PARADIGM

Our research found that most organizations surveyed are experiencing problems associated with the COVID-19 crisis, or they are undertaking practices that could lead to problems in the future. As shown in Figure 4, five out of nine organizations surveyed is in a jurisdiction that is currently subject to some type of lockdown order, such as those requiring citizens to stay at home or shelter in place. Moreover, two-thirds of organizations have seen an increase in helpdesk calls because their employees are adjusting to a new work-from-home paradigm that they previously had not experienced.

Figure 4
Current Practices Resulting 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%
Our workplace is in a jurisdiction that is currently subject to a "stay-at-home", "shelter-in-place" or similar order	55%
We are permitting employees to use their own devices (e.g., desktops, laptops, smartphones, etc.) when working from home	52%

Source: Osterman Research, Inc.

Figure 4 also reveals that slightly more than one-half of organizations are permitting their employees to use their own devices, including their home computers, to work from home, often because there is no corporate laptop or desktop computer for them to use. While the use of personal devices has been the norm for many years, this is a new phenomenon for millions of workers and will present numerous security and compliance challenges moving forward.

IT, SECURITY AND COMPLIANCE ARE SCRAMBLING

Organizations of all sizes are scrambling to support a suddenly at-home workforce. As shown in Figure 5, our research found that 70 percent of organizations are providing remote access capabilities for all employees who are working from home. Fifty-seven percent of organizations have deployed additional security measures, such as two-factor authentication and virtual private networks. However, fewer than one-half of organizations have undertaken other steps, such as deploying various security protections on remote devices, mandating password-protection on all web conference sessions, or providing additional security awareness training to work-from-home employees.

Two out of three organizations seen an increase in helpdesk calls because many employees are new to working from home

Figure 5
Capabilities That are Being Provided to Work-From-Home Employees

Issue	%
We provide remote access capabilities for all employees who are working from home	70%
We have implemented additional security measures, such as two-factor authentication, multi-factor authentication, virtual private networks (VPNs) etc. for employees accessing business systems and applications from home	57%
We have deployed security protections on employee devices used remotely, including mobile devices used to conduct business	44%
We have mandated password-protection on all web conferencing to prevent outside access to company communications	40%
We have rolled out additional security training to employees who shifted from working in an office to working from home	35%
We provide remote access capabilities only for some employees who are working from home	25%
We have mandated password-protection only for some web conferencing to prevent outside access to company communications	23%

Source: Osterman Research, Inc.

SOME THINGS ARE STILL GOING WELL

The survey asked IT decision makers and influencers how well various aspects of their communications and collaboration are going in the sudden work-from-home situation in which most find themselves. When asked to rate how well things are going on a seven-point scale that ranged from "very poorly" to "very well", 81 percent responded that their employees' ability to communicate with other employees and various others outside the organization was proceeding "well" or "very well". As shown in Figure 6, we also found positive results for other aspects of corporate communications, including the use of video meetings as a replacement for in-person contact, as well as replacing these face-to-face meetings with audio-only meetings. Low on the list was the ability for employees to share files with others and the general availability to equipment and various technology solutions.

Figure 6
Management of Communication and Collaboration Issues
Percentage responding "well" or "very well"

Source: Osterman Research, Inc.

THERE ARE SEVERAL CONCERNS

Not surprisingly, IT and security decision makers and influencers have a number of concerns about the current work-from-home situation. As shown in Figure 7, nearly one-half are "concerned" or "extremely concerned" about hackers attempting to take advantage of the sudden work-from-home situation for their employees and exploiting the potentially reduced security defenses that are available. More than one-third are this concerned about the potential for ransomware and/or phishing attacks delivered through email somehow compromising employees' endpoints. Other concerns, although further down the list, represent various and significant security, compliance and other risks.

IT and security decision makers and influencers have a number of concerns about the current work-from-home situation.

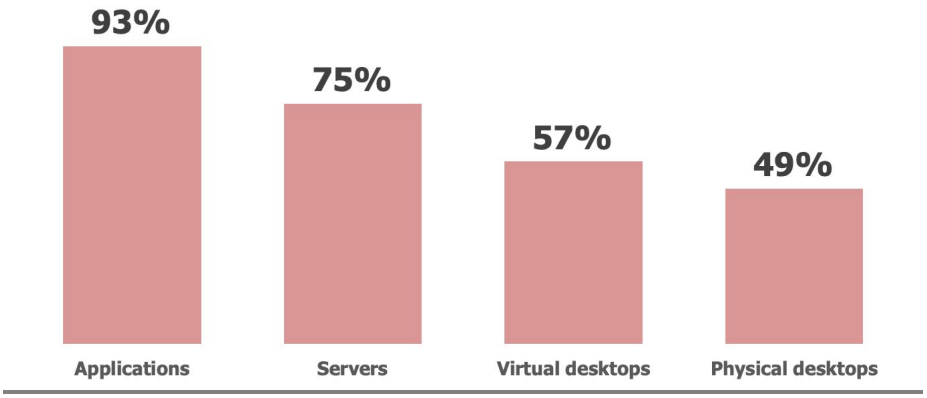
Figure 7
Concerns About Various Issues
Percentage responding "concerned" or "extremely concerned"

Source: Osterman Research, Inc.

EMPLOYEES NEED ACCESS TO KEY CAPABILITIES

As shown in Figure 8, almost all employees need secure, remote access to applications and the vast majority need access to corporate servers to access various data and other resources. More than one-half need access to virtual desktops and about one-half need some sort of a physical desktop computer to do their work.

Figure 8
Resources to Which Employees Need Secure, Remote Access
Percentage of organizations



Source: Osterman Research, Inc.

EMAIL CAPABILITIES NEED TO BE MAINTAINED

IT and security decision makers and influencers anticipate that email use for key processes will increase during the COVID-19 crisis. As shown in Figure 9, 95 percent of them believe that use of email for normal communications will either stay the same or increase during the crisis, while only five percent believe that email use for communications will decrease. Forty-four percent believe that use of email for sending files and documents will increase and nearly as many believe that the same level of demand for these services will be required.

IT and security decision makers and influencers anticipate that email use for key processes will increase.

Figure 9
Anticipated Changes in Use of Email Use During the COVID-19 Crisis Compared to Before the Crisis

Process	More	Less	Same
Email communications	64%	5%	31%
Sending files/documents	44%	13%	42%
Sending contracts/approvals	30%	25%	45%
Sales activity/contact customers, prospects	30%	35%	35%

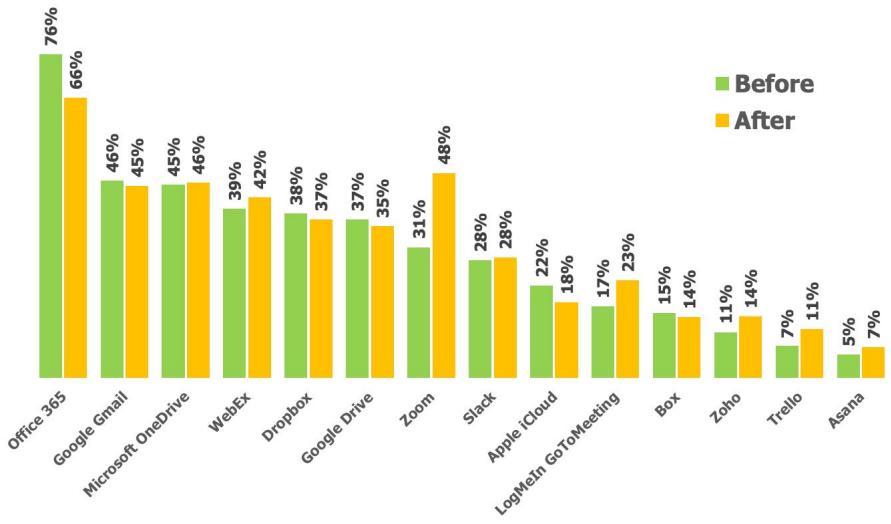
Source: Osterman Research, Inc.

What this tells us is that email will continue to be a mainstay during the crisis, and that in order for employees to remain productive, corporate email systems will need to be operating at a very high level – and certainly no less reliably than they do under normal circumstances.

USE OF APPLICATIONS HAS CHANGED

Our research found that employees will be using largely the same applications during the COVID-19 crisis as they did while working under more normal conditions, as shown in Figure 10. However, we are seeing a significant increase in the use of video meeting technologies that are in use to replace in-person meetings.

Figure 10
Use of Various Applications Before the COVID-19 Crisis and Now



Source: Osterman Research, Inc.

Interestingly, the figure above shows that use of Office 365 has decreased significantly for employees suddenly working from home. While that's odd given the reliance that most employees place on the use of the Office suite of tools, there are some possible explanations for this. It may be that because Office is used commonly in-home environments, many employees are using their personal copy of Office 365 or on-premises Office in lieu of their corporate license, at least in the early stages of their work-from-home experience as they get their other capabilities set up. Moreover, given that this survey was conducted in the early stage of many jurisdictions' stay-at-home and similar orders, many employees have been working from home only a short time and so are focused on replicating the in-person meeting

In order for employees to remain productive, corporate email systems will need to be operating at a very high level.

experience first, hence the increased use of Zoom, Microsoft Teams and other video-communication tools.

SECURITY NEEDS TO BE BOLSTERED

We found that 58 percent of the organizations surveyed are using cloud security services, among other solutions, to protect their newly homed workforce. Forty-three percent are backhauling all data to their corporate data center via full tunneling, and another 31 percent are doing so via split tunneling. However, as shown in Figure 11, one in six employees is estimated by IT and security decision makers and influencers to be bypassing on-premises, corporate security solutions.

Figure 11
Methods by Which Organizations are Providing (or Not Providing) Security Capabilities for Corporate Traffic
Percentage of organizations

Issue	%
We use cloud security services	58%
All traffic is backhauled to our corporate data center(s) via full tunneling	43%
All traffic is backhauled to our corporate data center(s) via split tunneling	31%
At-home users are bypassing on-premises, corporate security solutions	17%

Source: Osterman Research, Inc.

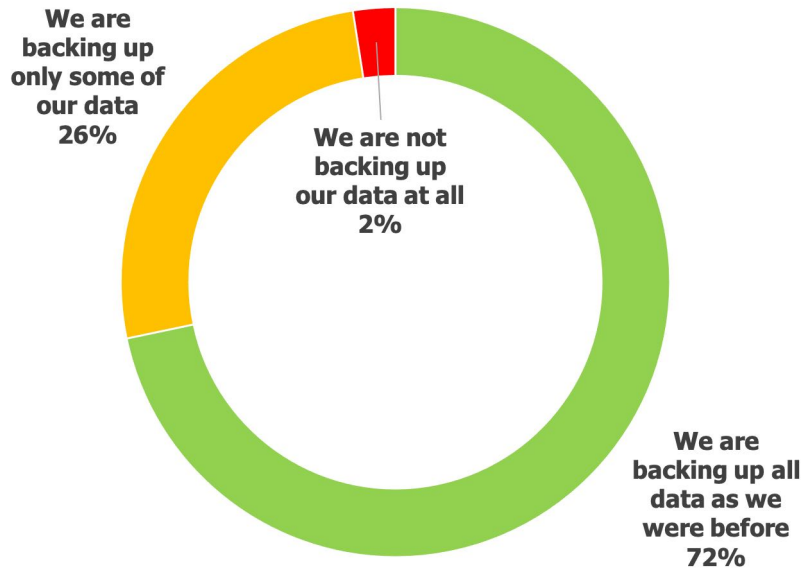
The fact that so many uses are bypassing on-premises, corporate security solutions is a major red flag for any corporate decision maker. Given that the vast majority of these users are less protected than they would be in an office environment, while also accessing corporate data and other resources, this creates an enormous level of exposure to various types of threats.

The fact that so many uses are bypassing on-premises, corporate security solutions is a major red flag for any corporate decision maker.

MOST DATA IS BEING BACKED UP

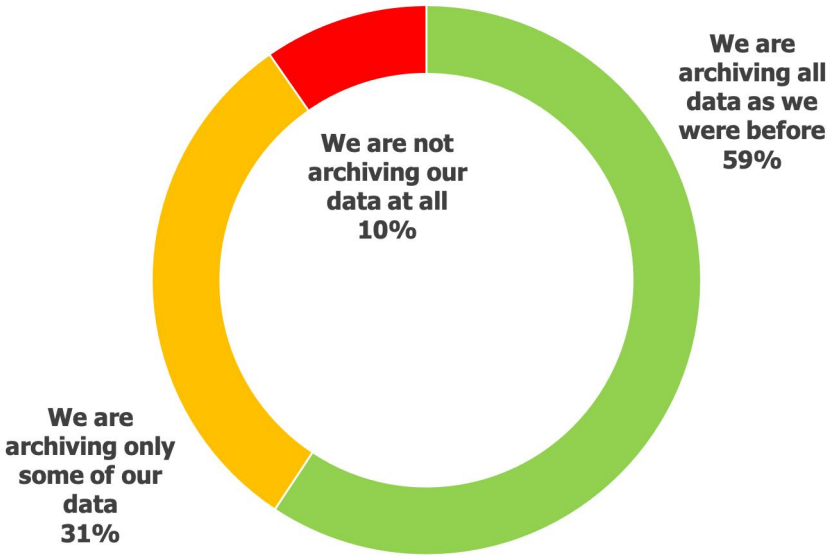
As shown in Figure 12, our research found that nearly three in four organizations are continuing to back up their data as they were before. However, about one-quarter of organizations are not backing up all of their data, and a small proportion are not backing up any data at all. Even worse, as shown in Figure 13, even fewer organizations are archiving all of their data as they were previously and 31 percent are archiving less than was the case before. However, one in ten organizations are not archiving their data at all.

Figure 12
Backup Practices During the COVID-19 Crisis



Source: Osterman Research, Inc.

Figure 13
Archiving Practices During the COVID-19 Crisis



Source: Osterman Research, Inc.

About one-quarter of organizations are not backing up all of their data, and a small proportion are not backing up any data at all.

This is a very serious issue from a compliance perspective. Even though employees are working from home and generating business records, processing customers' personal information, and carrying out other data-generating tasks under highly unusual and disruptive circumstances, that does not obviate their need to satisfy their

compliance obligations. The failure to archive all necessary business records during the period of the COVID-19 crisis is going to have long-term ramifications for businesses that fail to retain and protect their business records properly.

SECURITY AND COMPLIANCE ARE SUFFERING

As corollaries to the previous points in this section, Figure 14 shows that both compliance and security capabilities are now reduced during the work-from-home phenomenon. For example, while 64 percent of organizations report they agree with the idea that they were doing an excellent at job maintaining compliance with their various obligations before the COVID-19 crisis, that level of agreement has fallen to 56 percent now. Similarly, while 56 percent were in agreement that they were doing an excellent job at blocking security threats before, that figure has dropped to 49 percent today. Even under normal circumstances figures for doing an excellent job at compliance and security should not be this low, the current crisis has had a significant impact on organizations' ability to deal effectively with both.

Figure 14
Changes in Compliance and Security Posture Before and During the Current Crisis
Percentage responding "agree" or "strongly agree"

Issue	%
Before this crisis, we were doing an excellent job at maintaining compliance with our various compliance obligations	64%
During this crisis, we are doing an excellent job at maintaining compliance with our various compliance obligations	56%
Before this crisis, we were doing an excellent job at blocking security threats from impacting our organization	56%
During this crisis, we are doing an excellent job at blocking security threats from impacting our organization	49%

Source: Osterman Research, Inc.

Compliance and security capabilities are now reduced during the work-from-home phenomenon.

THERE ARE SOME ADDITIONAL PROBLEMS

The COVID-19 crisis has created some additional problems other than discussed previously, as shown in Figure 15:

- 46 percent of those surveyed are largely not in agreement that their remote access solution has scaled properly to cope with the additional workload from employees working from home.
- 52 percent of organizations don't agree with the idea that their existing security architecture effectively secures their remote workers as well as when they are in the office.
- 55 percent don't agree that their organization can properly recover from an attack directed against their organization.
- 59 percent don't really believe they have proper visibility into threats targeting their users.
- 38 percent believe that employees' home routers will create additional security risks for the organization.

Figure 15
Agreement With Various Issues
Percentage responding "agree" or "strongly agree"

Issue	%
Our remote access solution scaled to cope with the additional workload from employees working at home	54%
Our existing security architecture effectively secures remote workers similarly to in-office workers	48%
We are well-prepared to recover from an attack given the recent, significant rise in malicious activity	45%
We have visibility into threats targeting our users based around specific world events	41%
We were very well prepared for a situation like this in which our employees had to start working from home with very little notice	40%
Our employees' home routers will create additional security risks for our organization when used to access the corporate network and data	38%

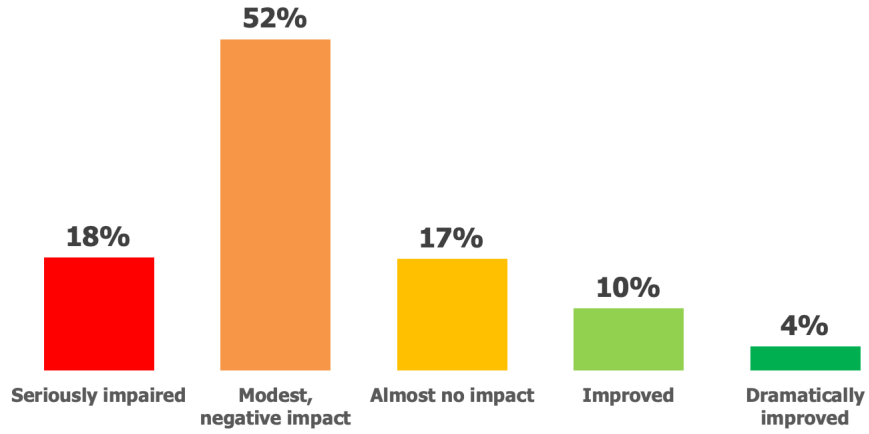
Source: Osterman Research, Inc.

MOST ARE BEING HURT BY THE CURRENT CRISIS

As shown in Figure 16, seven out of 10 organizations are experiencing a modest or serious negative impact from this crisis, as we would have expected. However, about one in six organizations have experienced no impact, and about one in seven are actually experiencing an improvement in normal operations because of the crisis.

Seven out of 10 organizations are experiencing a modest or serious negative impact from this crisis.

Figure 16
Impact of the COVID-19 Crisis in Terms of the Ability to Maintain Normal Operations

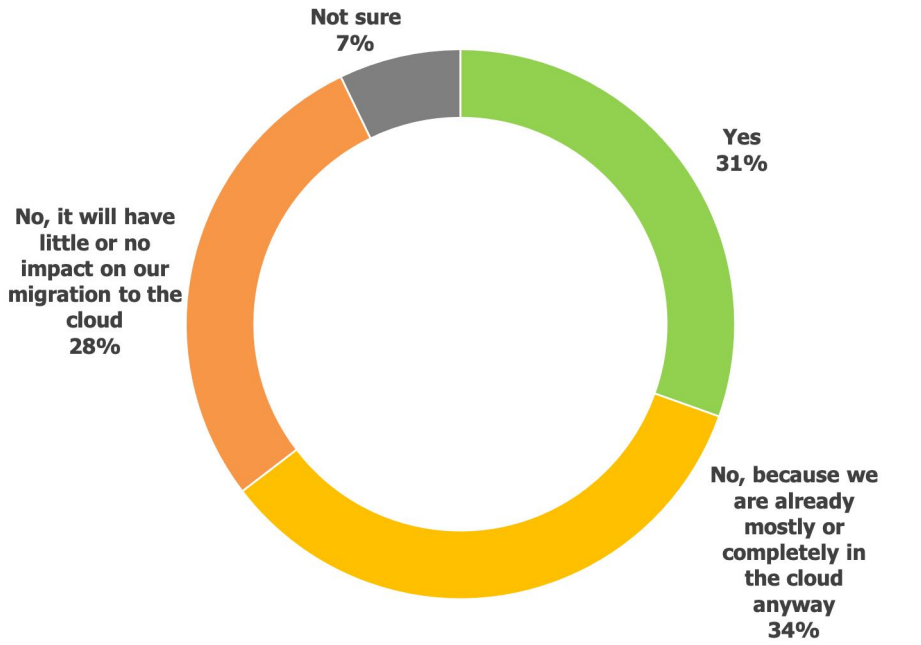


Source: Osterman Research, Inc.

THE CRISIS WILL ACCELERATE A MOVE TO THE CLOUD

We found that nearly one-third of the decision makers surveyed believe that the COVID-19 crisis will actually accelerate their organization's migration to the cloud – not a surprising result given the sudden, increased reliance on various cloud-based services to support a suddenly at-home workforce. As shown in Figure 17, another 34 percent of decision makers will not accelerate their move to the cloud, but only because they are largely there anyway. The final 35 percent either have no plans to move faster to the cloud as a result of the current crisis, or they just aren't sure of how it will impact this migration.

Figure 17
"Will the current situation accelerate your organization's migration to the cloud?"

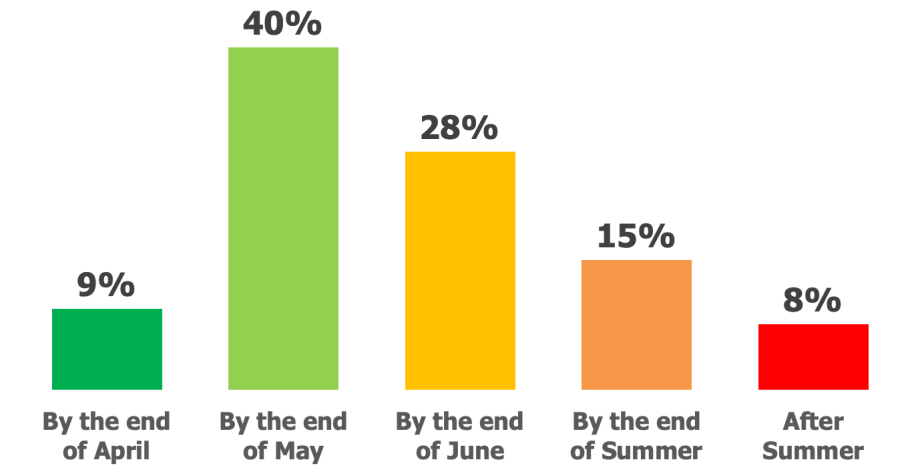


Source: Osterman Research, Inc.

WHEN WILL THE LOCKDOWNS END?

Nearly one-half of those surveyed believe that the various state, provincial and national lockdowns will end no later than the end of May 2020, as shown in Figure 18. Another 28 percent believe they will end by the end of June, while 23 percent believe they will end by summer or later.

Figure 18
"When do you expect this situation to be over and your employees will be working back in the office or wherever they normally work?"



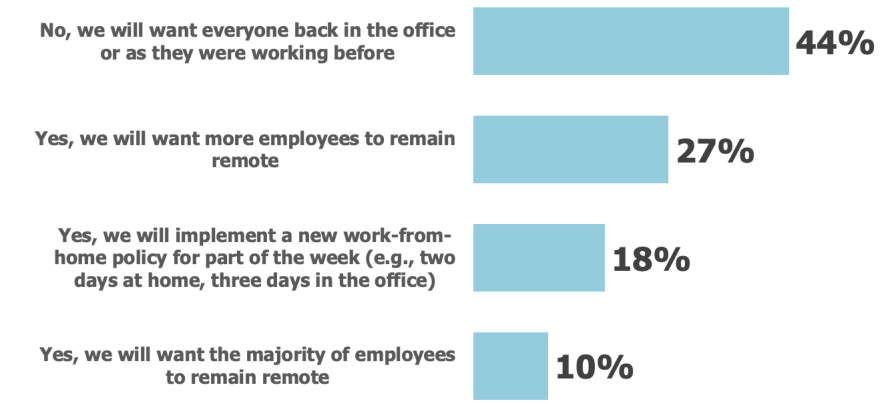
Source: Osterman Research, Inc.

Nearly one-half of those surveyed believe that the various state, provincial and national lockdowns will end no later than the end of May 2020.

THE LONG-TERM IMPACT ON REMOTE WORK

Many organizations surveyed believe that the COVID-19 crisis may very well have a long-term impact on the future of their workforce. As shown in Figure 19, 56 percent of organizations are seriously considering having more of their workforce work remotely. Nearly one-half of those in the "more remote workforce" camp will want more of their employees to remain remote after the current crisis is over, while about two-thirds of that number will implement some sort of work-from-home policies that will enable employees to work from home at least part of the time. A small proportion anticipate that they will want a majority of their employees to remain in permanently remote status.

Figure 19
"Do you think your organization will change your remote office work strategy once this situation is over?"



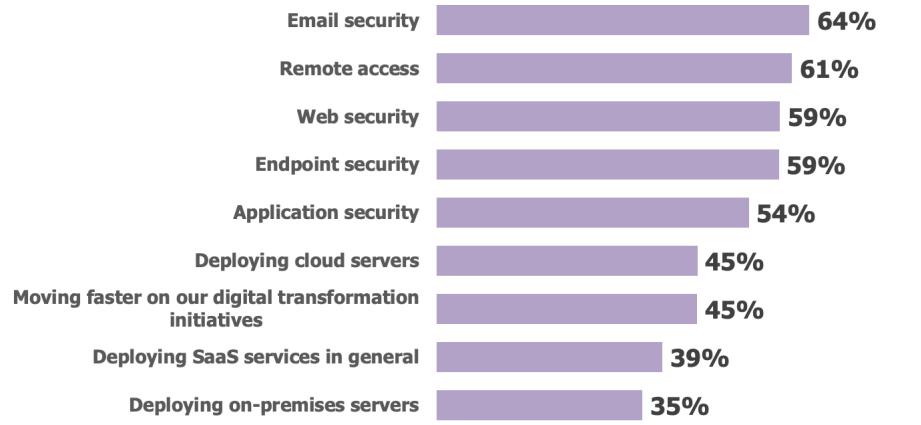
Source: Osterman Research, Inc.

PRIORITIES FOR FUTURE INVESTMENTS

The COVID-19 crisis has driven a number of organizations to place a high priority on a number of new or additional capabilities. As shown in Figure 20, nearly two-thirds of organizations give a "high" or "very high" priority to augmenting their email security capabilities, while another 61 percent place this high a priority on improving their remote access capabilities. However, a review of Figure 20 indicates that organizations want to augment a wide range of security and other capabilities in response to the current crisis. Along these lines, the three best practices for ensuring secure remote access is to strengthen security for IAM applications, VPNs and Virtual Desktop Infrastructures (VDIs), and secure access to physical endpoints/desktops.

The COVID-19 crisis may very well have a long-term impact on the future of their workforce.

Figure 20
Priority for Augmenting Various Corporate Capabilities
Percentage responding a "high" or "very high" priority



Source: Osterman Research, Inc.

Best Practice Guidance

Working-from-home a couple of days a week as part of a job role that's normally based in an office is a regular approach for fewer than 20 percent of employees. Some firms have designed themselves around a completely remote model with no central office and no co-location of employees, but these exceptions are few and far between. Both approaches to work design have emerged over the past 50 years as a counter-cultural way of working, but both have taken root within an overall stable ecosystem where the majority of people go to their place of employment during working hours. Additionally, several high-profile companies have cancelled working-from-home arrangements in recent years (e.g., Yahoo and IBM), for the stated reason that collaboration, communication and innovation happens best among co-located employees. These cancellations have given remote working a bad rap, particularly since the companies provide technology to enable remote working arrangements.

Being forced by government edict to suddenly transition an entire workforce to work-from-home arrangements under emergency conditions is an unprecedented and uncharted deviation from the norm of the past 50-70 years. As with any sudden, unplanned and unexpected change, working-from-home under emergency conditions is filled with many unknowns, for example:

- Do employees have appropriate physical spaces at home for working? For those in small apartments in major cities, along with those sharing home spaces with partners, children and other family members, the answer is often no.
- Do employees have appropriate devices, network connections and security software in their rapidly assembled, makeshift home offices to ensure that organizational security requirements, data protection mandates, and compliance obligations are still met?
- Will employees be more likely to fall victim to social engineering attempts – e.g., phishing messages – at a time of heightened fear (for personal health and safety), uncertainty (including job security and the degree of economic hardship they will have to face) and significant unknowns (when lockdowns will end, if remote family members are okay, etc.)?

Do employees have appropriate devices, network connections and security software in their rapidly assembled, makeshift home offices?

The lack of timeframe to make a planned and orderly transition to widespread work-from-home arrangements raises the need for clarity on how best to proceed. We offer the following best practices.

ENABLE USE OF SUPPORTED APPLICATIONS

Provide access to a catalog of supported and approved apps for business purposes which employees can work with and use from beyond the office.

Apps that have been researched, piloted, introduced and embedded in the normal working practices of an organization under standard operating conditions should continue to be used in work-from-home arrangements, if at all possible. This best practice rests on the belief that such apps support the security, compliance and risk frameworks under which the organization operates. In situations where employees can be given secure access to current apps – whether on-premises or delivered via cloud services – deviations from normal security and compliance approaches will be minimized.

If new apps need to be located and introduced under urgency to support work-from-home arrangements, then ensure the immediate gain of productivity isn't at the cost of unbearable pain later on due to security and compliance blunders. New apps should be selected in light of the classes of data that will be discussed, shared, stored and analyzed by employees, with higher levels of caution applied to any sensitive and confidential data (e.g., personal identity data, health information, financial data, etc.). There is a growing emphasis on finding apps that have been built with security and privacy as fundamental design considerations, rather than as an afterthought. Aspects to look for in any new apps include:

There is a growing emphasis on finding apps that have been built with security and privacy as fundamental design considerations.

- Support for current corporate authentication approaches so that employees don't have to create separate accounts with different authentication credentials. Authentication approaches like hardware security keys, should be proven to be highly phishing-resistant and offer strong protection against account takeovers, while being fast and easy to use.
- End-to-end encryption based on strong encryption standards.
- Controls over what people external to the organization can see and do within the app. With video meeting apps, for example, ensure appropriate restrictions exist to limit when external participants can join a meeting. With file sharing apps, on the other hand, perhaps external participants should only be able to view a document rather than edit or download it too.
- The geographical locations through which corporate data is routed, processed or stored. Modern data protection legislation, such as Europe's GDPR, seeks to limit data transfers to jurisdictions beyond Europe, and many governments and organizations are concerned about inadvertent risks to data sovereignty when data is stored in foreign countries.
- Integration with current archiving, backup and monitoring tools. A lack of integration means essential records are lost, evidence is not captured, and disaster recovery is not possible. Separate archiving and backup approaches multiply complexity and increases the attack surface for data breaches via archival and backup repositories.
- Certified adherence to the normal data protection standards for your industry or market sector, such as financial services, healthcare, education, and where the data of children is being processed.
- The use of monitoring technologies to monitor the employee experience enables the help desk to be both proactive and reactive.

The corollary of this best practice is to beware the use of inappropriate, unsecured apps for business purposes while employees work-from-home. Many apps that support and enable remote working have posted huge growth numbers during March 2020:

- Some apps have never been ready for business. For example, WhatsApp's usage increased 40 percent from February to March 2020, but from a security and compliance perspective, WhatsApp's own terms and conditions prohibit business usage.

- Other apps come from vendors with a history of questionable data protection practices and recent significant data breaches, e.g., Facebook. In addition to the growth of WhatsApp, Facebook also said that group calls in Facebook Messenger increased by more than 1,000 percent over the same one-month period.

- Still other apps that experienced solid growth in business markets before the COVID-19 pandemic have been undermined by revelations of compromised security as usage has exploded. Zoom is the poster child of this class of apps, with usage increasing from 10 million to 200 million monthly active users, in parallel with the identification of a litany of security problems including compromised encryption standards, traffic routed through China for no apparent reason, poorly structured and breach-prone file names for meeting recordings, and easily guessed meeting IDs leading to uninvited participants joining calls (or "Zoombombing"). Firms, educational districts, and the governments of several countries have banned the use of Zoom in response. It's hard to foresee that Zoom's public repentance over its security shortcomings and promises to do better will flow through to a hardened security design during the current pandemic crisis.

The use of non-corporate email on personal devices for business purposes is another threat vector to watch out for. Sending and receiving business email messages via a personal account on a device that's shared with other home members creates a situation ripe for unauthorized access to business data, and additionally, if the account is compromised through a phishing attack, business content will be breached by the attackers.

The use of non-corporate email on personal devices for business purposes is another threat vector to watch out for.

STRENGTHEN IDENTITY AND AUTHENTICATION

With compromised account credentials being the leading factor in the majority of data breaches, it's time to stop using authentication that relies on a username and password pair. Phishing attacks steal credentials. Brute-forcing passwords identify the presence of weak and ineffectual passwords in cloud and on-premises directories. And data breaches have revealed millions of username and password combinations in recent years, which are available for purchase by wannabe cyber criminals. Something much greater is needed to protect corporate data, limit access to sensitive and confidential information, and safeguard employees from phishing and other cyber attacks. This is particularly the case when employees are working away from the office on a range of non-corporate devices and networks (hence reduced security protections), and the fear and uncertainty of the pandemic elevates the likelihood that people will fall for social engineering attempts with COVID-19-related content.

This best practice is to strengthen current identity and authentication approaches, including moving away from a reliance on passwords. Aspects include:

- Passwordless authentication using biometrics for greater identity security. Passwordless authentication uses an architecture based on public key cryptography and secure enclaves on local devices to store the private key. A PIN number, fingerprint or face scan unlocks the private key, but this never leaves the local device and without it the public key cannot be used to authenticate to other services.

- Multi-factor authentication (MFA) for all employees and all systems, with stronger forms of MFA greatly preferable over the easier approaches that have proven more vulnerable to compromise. SMS codes to a smartphone should be avoided (due to targeted social engineering attacks that steal SIM credentials), and likewise sending a one-time code to an email address should be avoided (in case the email account is already compromised). Authenticator apps, such as Google Authenticator, have also been compromised through carefully constructed attack sequences, and while these attacks have been few and far between, they have not proven attack resistant. Employees and senior executives dealing with sensitive and confidential information would be best to limit usage of authenticator apps. The most secure approach to MFA - and the fastest - currently relies on public key cryptography and the use of hardware token devices using the FIDO U2F and FIDO2/WebAuthn standards.

- Connecting all supported apps to a centralized identity and authentication service for single sign-on in order to eliminate credential proliferation. One corporate identity and strong authentication approach can be used to gain appropriate access to all corporate apps. This creates immediate productivity benefits for each employee on a day-to-day basis. It also benefits the organization strategically because both employee terminations and job role changes within the organization are easily enforced through centralized updates.

- Monitoring authentication requests with behavioral analytics to highlight abnormal patterns and probable compromised credentials, such as multiple near-time logins from different geographical areas (which should be non-existent during lockdowns and strident travel restrictions) or from countries in which employees are not working. Abnormal requests can be blocked outright, or additional identity verification demands enforced before access is granted.

Strengthened authentication should even be enabled for employees calling into organizational services for remote assistance, including human resources and the help desk. Many fewer implicit authentication signals are available to such groups when people are working from home, such as office extension numbers and on-network activity. If account credentials have been compromised, HR and help desk staff may be tricked into providing sensitive information or verifying a new device for a threat actor rather than a real employee.

EXTEND THREAT PROTECTION

While much of the world has been in lockdown and unable to work as normal, one group of "workers" have taken advantage of the situation to step up their activity. Unfortunately, this group is composed of cyber criminals who use phishing and spear-phishing messages to install ransomware, spread malware, and steal account credentials. The governments of the United States and the United Kingdom issued a joint warning on the increase in phishing attacks tied to COVID-19 messaging, including the distribution of the $2 trillion stimulus package in the United States. Attackers have gone as far as creating exact copies of official White House web sites to trick users into downloading malware. Additionally, many threat protection vendors have observed similar growth in COVID-19-related phishing attacks across their threat intelligence infrastructures.

Extending threat protection capabilities to work-from-home locations and non-corporate devices used by employees for organizational purposes is a best practice. This includes:

Extending threat protection capabilities to work-from-home locations and non-corporate devices used by employees for organizational purposes is a best practice.

- Scanning email traffic for malicious links and documents, including pre-delivery link and document checking, and post-delivery real-time checking to ensure links and documents haven't been weaponized after delivery.

- Using behavioral analytics to verify email traffic patterns, as part of identifying impersonation attempts and the use of lookalike or soundalike domain names to trick employees into visiting malicious web sites. It's happening against high-

profile organizations during the COVID-19 pandemic: for example, cyber attackers targeted the World Health Organization (WHO) with a malicious web site that impersonated WHO's email infrastructure, in an attempt to steal account credentials from employees.

- Early warning of potential attack vectors through threat intelligence and domain impersonation registrations.

The corollary of this best practice is that it's no good if current email security and web security solutions for threat protection work only in the office environment. If current tools are unable to support employees and devices beyond the network, look for more scalable and broad reaching solutions.

HARDEN DEVICES

While many organizations have equipped employees with laptop computers to support work mobility across office, metro and global environments, many office-bound machines still exist. In sudden work-from-home situations, employees are likely to use current home computers for work purposes, especially if they offer larger screens than their work-issued laptop. This raises significant concerns and threat vectors for the organization, including:

- Operating system and application software vulnerabilities due to a lack of patching on home computers.
- Devices already compromised through persistence malware.
- Synchronization of corporate data through file sync and share clients that remain on the device even after the COVID-19 lockdowns have ended.
- Access to corporate data, apps and services stored on or accessible through the device by other people who live at or have access to the employee's home environment.
- Data created, stored or saved locally on the device will bypass current archiving and backup solutions.

It's no good if current email security and web security solutions for threat protection work only in the office environment.

The best practice of hardening devices is designed to ensure in-situ security vulnerabilities do not flow through to compromise corporate data, apps and systems. Options for hardening devices include:

- Providing a security awareness training module on the need for updating operating systems and application software to eliminate security vulnerabilities. The vendors of the dominant desktop and mobile devices offer regular updates and patches, and these should be enabled for automatic installation.
- Enrolling the home devices of any employee or executive that handles sensitive, confidential or personal data belonging to the organization in the endpoint protection platform (EPP), through the installation of an endpoint agent. Once installed, the agent works with the EPP to assess and verify the security stance of the device, including options for remedying any new weaknesses or vulnerabilities before access is granted to corporate data resources (whether on-premises or in the cloud).
- Employees who are unwilling to accept the installation of corporate security software on their devices - and for personally owned devices they have that prerogative - and if a hardened corporate device cannot be supplied for the employee's use, then a containerized or virtual desktop environment is the next best alternative. Such an approach provides secure access to corporate apps and data without installing any of this data on the employee's home computer or device.

The corollary to this best practice is that employees' offices may contain security threats that remain unseen by the organization, with smart speakers and other voice-activated digital assistants among the prime suspects. Several incidents over the past year where Amazon Alexa shared confidential data has raised concerns around the eavesdropping potential of Amazon's speaker. A recent research study found that smart speakers activate inadvertently up to 19 times a day. With new work-from-home arrangements being suddenly required to address the COVID-19 threat, several law firms advised staff to be careful when discussing client matters at home, including recommendations to check the default settings on Alexa, mute or shut off listening capabilities during the work day, or to turn such devices off entirely. Without the ability for an organization to see what other devices employees have in their home offices, raising awareness of the potential threats through a security training module is essential.

VERIFY AND SECURE NEW NETWORKING INFRASTRUCTURE

A corporate office environment gives an organization a high degree of control and certainty over its networking infrastructure, including approved brands, standard configurations, vulnerability analysis, patching levels, firewall restrictions, and even rules on the types of devices that can connect. In a sudden work-from-home situation, as currently experienced with COVID-19 lockdowns across the world, this control and certainty is eliminated. Employees are using their current home broadband routers and Wi-Fi equipment, and provenance, security status, misconfigurations, and the presence of other already compromised devices on an employee's home network are entirely unknown.

This best practice calls for checking the security status of current home networking infrastructure, and addressing security vulnerabilities through patching, replacement, or circumvention. Approaches include:

- Request that employees change the factory default password on their home router, and if this has already been done some time previously, to change it again to reduce the likelihood that an unauthorized actor has control over its settings. Poor security of home routers has already been used to stage a COVID-19-themed attack. After locating vulnerable home routers, the cyber attackers changed the DNS settings to redirect traffic meant for particular websites to ones they controlled. The malicious websites offered a COVID-19 informational app download that actually installed data stealing malware.

- Offer a fast-track method for employees to check the security status of their home router and configuration, along with instructions on how to update to the latest configuration files. If employees' current routers are vulnerable to compromise and the associated vendors have not released security updates, employees handling sensitive and confidential data should consider upgrading to more secure models. A recent study by the American Consumer Institute found that over 80 of Wi-Fi routers in U.S. homes and offices had security vulnerabilities due to outdated firmware.

- Avoid the use of free public Wi-Fi networks, which can be compromised by malicious actors in numerous ways to enable malware distribution, credential compromise, and data theft.

Request that employees change the factory default password on their home router.

MONITOR WHAT'S GOING ON

Most conventional monitoring solutions focus primarily on the infrastructure supporting a specific service or application. In an on-premises scenario, there is normally a good understanding of what each piece of the infrastructure is responsible for, the relation between components, and what normal behavior looks like for each component. In practice, however, this approach proves to be much less effective with cloud-based services, especially in the sudden work-from-home scenario when many new cloud applications are hitting networks for the first time.

In a cloud-based system, visibility is limited and the relationships between key system components are mostly unknown, and cloud providers typically don't share much information about how things are working. Microsoft offers the Service Health Dashboard, but this is not updated very often and is not easily available outside of Office 365 Administrators. Moreover, the massive scale of a cloud service, such as Office 365, coupled with the way users are distributed across several datacenters and hundreds of thousands of servers, makes it almost impossible to maintain the same monitoring paradigm. Administrators simply cannot correlate what information is relevant to their organization and what isn't, in part because they don't have all of the information they need about all of the components.

There are fundamental differences between how an on-premises application or a cloud-based system are managed, and so an entirely new monitoring approach is required. Cloud-based systems enable organizations and users to work from virtually anywhere, which is an enormous benefit for the new work-from-home paradigm. Because of this, monitoring a service from a specific location, typically the organization's datacenter, no longer represents how applications are used in the real world. Additionally, modern workplace teams are now tasked with providing training to reduce the learning curve for employees that are using cloud-based systems. The desire is to increase organizational productivity through the use of new innovative cloud-based systems.

Instead, the customer-centered approach to monitoring cloud services maintains a strong focus on measuring and reporting on the employee experience. The modern, customer-centered approach injects probes into the locations that the customer specifies to carry out typical end-user tasks and reports back on performance. These employee experience probes provide the necessary data and resulting analytics to ensure complete visibility into performance and service quality at each individual location. Monitoring the experience that employees have through synthetic tests when using a cloud service is critical to identifying and localizing problems. After all, the ultimate measure of any cloud-based service is whether or not the service is available for employee consumption.

Fundamentally, administrators must be able to determine what caused an outage or service slowdown so that they can respond properly to issues that come up, and so that they can minimize the time required to resolve an issue. This is especially critical given the reliance on cloud applications to support work-from-home employees. Customer-centered monitoring that leverages end-user experience probes, along with real-time synthetic tests, are critical in determining where the problem lies. In the absence of modern monitoring capabilities, quickly understanding where problems are occurring and who is affected may not be possible.

Sponsor of This White Paper