Department of Transformation and Shared Services
Governor Asa Hutchinson
Secretary Amy Fecher

Cyber Security Data Center Modernization Proposal

CARES Act Steering Committee
Submitted by: Department of Transformation and Shared Services

The pandemic has created an immediate need to standardize, stabilize, and secure state systems to improve cybersecurity efforts. The Department of Transformation and Shared Services (TSS), Division of Information Systems (DIS) requests funding to centralize and modernize the information technology infrastructure for all executive branch state Departments.

Cybersecurity is a critical area for investment in this project. The cyberattack surface has greatly expanded as the workforce has evolved into a "work from anywhere" model due to the pandemic.. TSS DIS has seen a dramatic increase in Cyber threat activity over the past year and this continues into 2021 and beyond. Investment into Cyber Security and Risk Management is critical to the continued mission success of our State Government.

Technology transformation moves slowly at the state-level because of funding and prioritization. Many of our data systems are suffering from old age and end of life status. The pandemic and remote work created additional stress on these systems and networks—revealing a series of vulnerabilities. This aging and de-centralized infrastructure leaves the state vulnerable. These older systems lack a process for updates and patches and have no security control standards in place

This funding will also be utilized to create a uniform statewide disaster recovery solution that will provide failover capability for critical state information systems to ensure continuity of business operations in the event of a system failure or data breach. The state will be able to maintain a remote access framework that is accessible and secure and will support remote work operations, as necessary.

NOTE: You will find articles attached to this proposal that indicate the need for heightened cyber security with the increase in remote workers and how other state governments are accessing CARES Act funding to boost their cyber security needs.

An outlay of $33.5M will allow the state to purchase equipment, software, and services necessary to optimize the stability and security of state technology operations, especially when engaging in remote work and access. This modernization will position the state information systems to take advantage of cloud computing opportunities while preserving state control over data and systems.

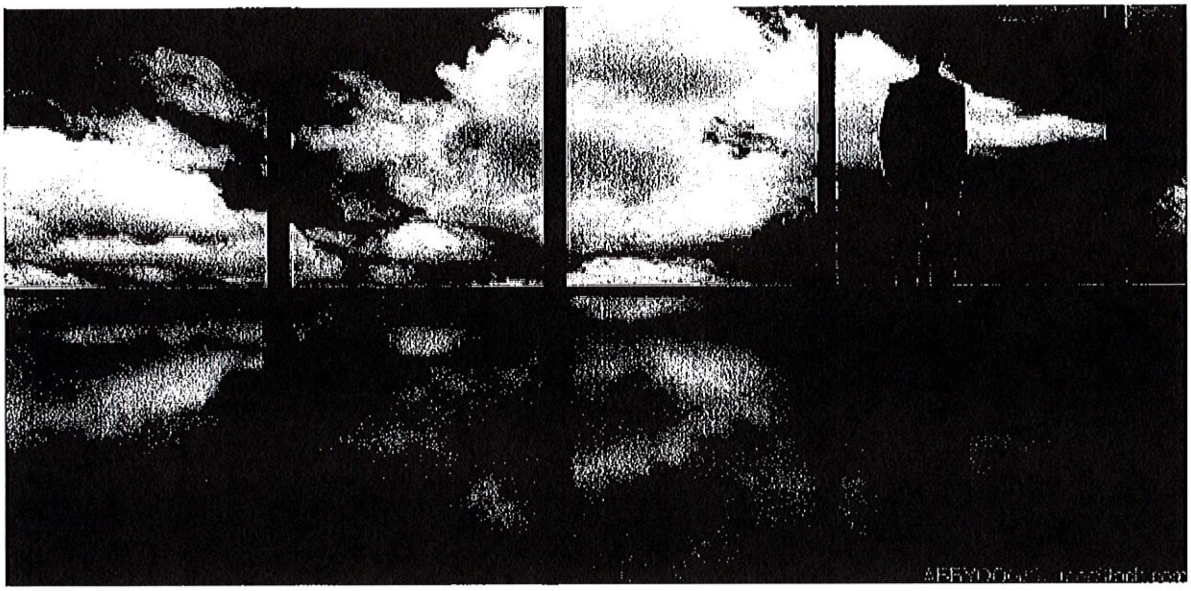
TSS DIS is requesting **$33.5M** to upgrade information technology infrastructure and engage third-party vendors to the extent necessary to improve cybersecurity, modernize infrastructure, and ensure continuity of operations for all state Departments.

Build of Materials (BOM)	**Cost with Managed Services**
Network and Security BOM	$8,500,000.00
DIS Hosting BOM	
Server Hardware	$3,200,000.00
Storage High I/O	$3,150,000.00
Storage Mid-Low I/O	$4,520,000.00
Automation Software Set	$1,200,000.00
Replication Software (VM)	$750,000.00
Replication Software (AIX)	$250,000.00
Replication Software (x86)	$150,000.00
Backup Software	$2,000,000.00
Backup Server	$45,000.00
Backup Storage	$4,200,000.00
Infrastructure Monitoring	$1,750,000.00
Application Monitoring	$1,033,200.00
Patch Management	$450,000.00
Existing Virtualization Licenses	$2,250,000.00
Hardware and Software Subtotal	**$33,448,200.00**

Attachments:

1. Why Local Governments Should Secure CARES Act Funding (and how they can)
2. Prioritize, Navigate, Execute: State and Local Governments Invest CARES Act Monies in Critical IT Initiatives
3. How the Shift to Remote Working has Impacted Cybersecurity
4. The Cybersecurity Implications of Working Remotely

GCN



INDUSTRY INSIGHT

Why local governments should secure CARES Act funding (and how they can)

By Doug Harvey

Aug 11, 2020

Digital transformation moves slowly at the state and local levels, partly because it is not adequately funded or prioritized. The effects have been plain to see during the COVID-19 pandemic as unemployment offices, motor vehicle registries and local health departments have failed to keep up with the surge in requests. For many state and local agencies, technology infrastructure was considered a future expense, rather than a necessary investment.

With the Coronavirus Aid, Relief, and Economic Security Act (https://home.treasury.gov/policy-issues/cares/state-and-local-governments) (CARES Act), the federal government is helping cities and counties address this investment gap. The bill earmarked $150 billion for states and local governments responding to immediate pandemic-related needs of residents, including advancing lagging digital transformation efforts. The funding can help them replace outdated hardware and software with systems that are more resilient, scalable and secure in key areas such as:

> **Modern, cloud-based apps and infrastructure.** The pandemic has made many local governments realize that their legacy systems were not built with modern needs in mind. They are not equipped to scale with demand or designed to enable business as usual from remote locations. Local governments can address both issues with modern, cloud-

based solutions. A modern infrastructure, for example, is software-defined, virtualized and decentralized. This gives governments the flexibility, scalability and operational efficiency required to address residents' needs in real-time, from anywhere.

Digital-first for the workforce and residents. When offices were forced to close, many local governments were unable to conduct business without physical access to legacy systems, holding up everything from building permits to license renewals and access to land records. Digital workspaces can allow for a more flexible and remote workforce, and citizen-facing web applications can enable residents to access critical services and documents online and use contactless payments for items like parking tickets and renewal fees.

Security for all. Data and modern applications live in increasingly sprawling and distributed IT environments, and network users are no longer neatly contained behind perimeter firewalls. A **recent survey (https://www.carbonblack.com/resources/global-threat-report-extended-enterprise-under-attack-usa/)** by VMware Carbon Black found that cyberattacks and breaches have increased significantly during the COVID-19 pandemic due to employees working from home and COVID-related malware. Since state and local governments are tasked with securing sensitive resident data and must ensure the proper protocols, cybersecurity efforts must now encompass more than just core infrastructure and extend protection to the cloud, user identity and a variety of devices. While IT infrastructure upgrades can streamline services and reduce costs, they must also minimize the inherent risk of cybercrime.

While the opportunities for state and local governments are obvious, accessing CARES Act funding has proved challenging for some. Based on my conversations with state and local officials across the country, most mid-sized cities are taking the right steps to speed up their digital transformations with help from the CARES Act. But many smaller cities are being left out, either because they do not know what resources are available to them or how to apply for such benefits.

The Treasury Department **released guidance (https://home.treasury.gov/policy-issues/cares/state-and-local-governments)** to assist local governments in determining which expenses qualify for the Coronavirus Relief Fund, but cities and counties must keep three things in mind:

Expenses must be deemed necessary due to the COVID-19 public health emergency. IT investments that address resident needs and enable cities to provide key services apply.

Expenses must not have been included in a city's most recently approved budget. In other words, expenses must be for net-new expenditures that were not previously planned.

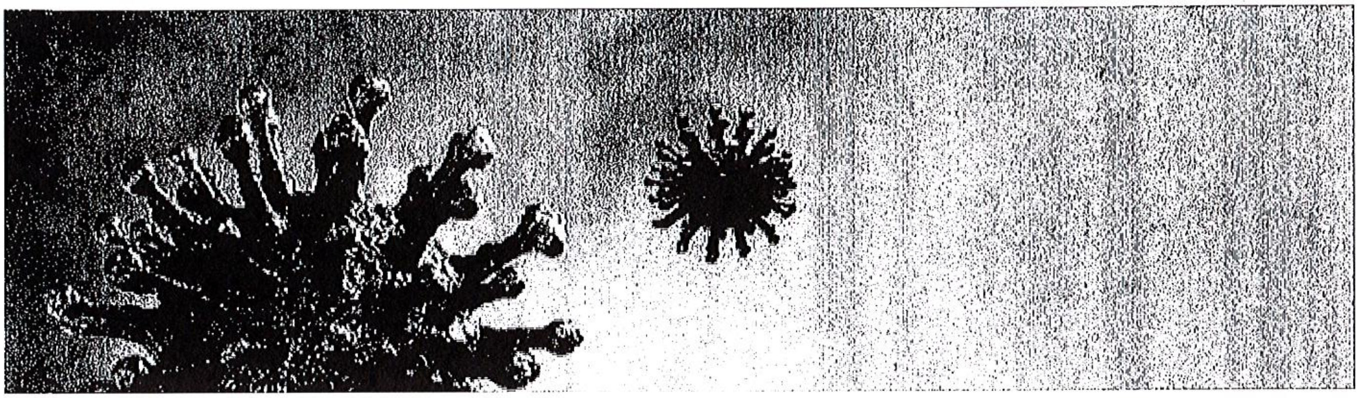
Local governments must move quickly to secure CARES Act funding. Expenses to the Coronavirus Relief Fund must be incurred by Dec. 30, 2020.

Cities and counties that need help can consult with IT organizations to determine which investments will have the most impact. These partners can also help agencies implement new infrastructure quickly to address the shortfalls of legacy systems and meet the needs of residents.

Digital transformation is a necessary investment for state and local governments, but it has been held back for too long by limited budgets and competing priorities. During the pandemic, we have seen how outdated IT infrastructure can wreak havoc on states, counties and municipalities and affect their ability to provide services. State and local governments should invest in their futures now before another opportunity passes.

About the Author

Doug Harvey is head of U.S. state and local governments and education for VMware.



INDUSTRY NEWS (HTTPS://WWW.MERITALKSLG.COM/NEWS/INDUSTRY-NEWS/)

Prioritize, Navigate, Execute: State and Local Governments Invest CARES Act Monies in Critical IT Initiatives

BY: GAIL EMERY (HTTPS://WWW.MERITALKSLG.COM/AUTHOR/GEMERY/) SEPTEMBER 2, 2020 | 10:49 AM

SHARE THIS STORY

After Congress passed and President Trump signed the nearly $2 trillion Coronavirus Aid, Relief, and Economic Security Act (CARES) in March to fight the harmful effects of the COVID-19 pandemic, billions of dollars began flowing down to state and local governments through a variety of funding streams – many existing, and some new. The funds support public health, schools, businesses, transit systems, residents in need, and more.

State and local governments – reeling from the one-two punch of unbudgeted expenses related to the coronavirus and declining tax revenue due to business closures and rising unemployment – eagerly anticipated the funds. Government leaders also found themselves in a sprint to understand the new funding streams, set up new offices and processes for distributing grant funds, and ensure the new Federal monies are spent in the allotted timeframe, which varies from program to program funded by the CARES Act.

"It's a learning curve for the full community – procurement teams, program managers, and IT – to become aware of all of the funding channels. Almost every grant has some IT component, even if it's tracking the grant itself," said Tony Powell, chief strategist and innovation officer for state and local government at Dell and a former CIO for the departments of Health and Revenue in Florida.

"The CIO is often not included in departmental budget conversations within states and municipalities," Powell added, "so it's very important for the CIO to know how grant dollars can be accessed and for what purpose, so they can compete for those dollars. Often, they may be deploying technologies that grants can pay for, but they don't see the connection."

Matt Pincus, director of government affairs at the National Association of State Chief Information Officers, noted that governors "are treating this funding as emergency funding, and they may not consider their IT environment an emergency function. CIOs need to make the case for why IT is so important right now and why governors should be allocating Federal resources to it."

Procurement teams and program managers can leverage funds for a myriad of IT uses – including improving and evolving the remote work environment, strengthening data protection, and modernizing data centers to create flexibility and efficiency. Powell recommends collaborating with IT to prioritize and select solutions that will provide long-term benefit.

The Feds deliberately funneled money through existing grant programs where possible to speed delivery of funds for critical relief efforts, Powell said. Even so, state and local governments are scrambling to avail themselves of multiple funding streams simultaneously. "Grant applications are typically spread throughout the year," said Eminence Griffin, senior manager for government affairs at Dell. "Now, all of these grant processes are happening at once. Keeping up with the new deadlines and processes, while addressing the pandemic, has been quite challenging."

Among the CARES Act funds (https://www.nlc.org/sites/default/files/users/user52651/Summary%20CARES%20Act%20FINAL.pdf?_ga=2.169790881.1402459149.1585593052-952051433.1568143774), Powell identified these as most important for state and local governments:

- The Coronavirus Relief Fund (CRF), a $150 billion grant program for states, territories, local and tribal governments. Funds must be spent on pandemic response activities between March 1 and Dec. 30, 2020, that were not already budgeted. Funds were distributed by the U.S. Treasury to states and to municipalities with more than 500,000 residents, based upon population. States could distribute funds to municipalities with less than 500,000 residents, but were not required to do so;
- The Federal Aviation Administration's Airport Improvement Program, which received $10 billion to maintain operations and respond to COVID-19 at the nation's airports, which are typically managed by municipal governments; and
- The Department of Health and Human Services' Public Health and Social Services Emergency Fund, which includes $100 billion for grants to hospitals, public entities, not-for-profit entities and Medicare- and Medicaid-enrolled suppliers and institutional providers to cover unreimbursed healthcare-related expenses or lost revenue as a result of COVID-19. Myriad activities can be supported by these grants, from medical licensing to contact tracing to staffing, all of which require technology support, Powell noted.

Step One in Pandemic Response: Prioritizing Needs

One of the biggest challenges state and local governments face is in prioritizing their needs, Griffin said. Dell encourages its state and local government customers to work with the company's strategists to evaluate their needs, explore technology solutions, and identify funding sources.

"They're trying to solve so many problems at once, whether it's telework, telehealth, or remote learning," Griffin said. "We want to provide as much information as we can to help them make the best decisions for their communities."

When the pandemic hit, Summit County, Ohio, immediately focused on enabling work from home. Then, it prioritized investments that would drive process improvement and long-term budgetary savings, said Brian Nelsen, chief of staff for County Executive Ilene Shapiro. Officials quickly identified virtual proceedings as essential to getting the courts running safely again.

Discussions between the county and the City of Fairlawn resulted in a plan to expand FairlawnGig, a municipal broadband utility established by Fairlawn in 2017, to create a secure and dedicated fiber-optic network for county and City of Akron municipal buildings that hold criminal justice proceedings or house inmates. The network will be used to enable secure, remote meetings and court proceedings. In mid-August, the Summit County Council approved a grant agreement with Fairlawn that will send $6.5 million of the county's $94 million in CARES Act funds to Fairlawn to fund the expansion. The project is expected to be complete in December.

Step Two: Addressing the Nuances of the Coronavirus Relief Fund

The CRF in particular presents three pressing challenges, state and local government leaders said:

- Spending the money by Dec. 30;
- Ensuring the money is spent only on activities that were not previously budgeted; and
- Ensuring that local governments with less than 500,000 residents receive a piece of their state's CRF funds.

The spending timeline is the biggest challenge, said Ana Bradshaw, COVID-19 financial and performance executive liaison for the City of San Antonio. A five-month timeframe for some technology projects is ambitious under normal circumstances, she noted.

San Antonio received $375 million in Federal grant funds, $270 million of which came from the CRF. To accommodate needed investments that require funding past Dec. 30, "We've leveraged that [CRF] grant funding to offset some of our city operating expenditures in public health and emergency medical response and create capacity in the city's general fund, which we can roll over from year to year," Bradshaw said.

Because the CRF requires that funds are spent on activities that were not already budgeted, many attorneys at the state level had very narrow interpretations of allowable uses, Pincus observed. "We heard from Treasury and from Congress that everything had to be prospective – it couldn't be used to backfill state budget gaps," he said. He hopes that any future stimulus bill will include a clarification that allows broader use of stimulus funds.

Because of the restrictions on allowable expenses, state and local governments have closely scrutinized investments with CRF funds. Before embarking upon the FairlawnGig expansion plan, Nelsen and Shapiro talked numerous times with Ohio's senators, the governor's office, the state auditor's office, the National Association of Counties, the County Commissioners Association of Ohio, and the state Office of Budget and Management to ensure the plan would align with CRF requirements.

"With this project, there is a clear line to court operations, which have ground to a halt during this period," Nelsen said. "In our opinion, this one is a no brainer in terms of CARES Act eligibility. We also believe this is a really good application of those funds in terms of the return on investment for taxpayers. Anything we can do to help us operate efficiently and control costs in the post-COVID environment is important."

Cybersecurity is an especially critical area for investment, as the cyberattack surface expanded exponentially as workers began working from home and bad actors seized upon the chaos of the pandemic onset to target government offices and healthcare organizations. The need for end-user cybersecurity training has never been greater, IT experts agree, but many counties have questioned whether they can spend CARES Act funds on phishing testing and cyber education, because many had already allotted funds for this purpose, said Rita Reynolds, chief technology officer for the National Association of Counties.

Beyond training, however, many other protections are needed to keep the newly remote workforce and government networks secure, such as multi-factor authentication, endpoint detection, and encryption. CARES Act funds present a great opportunity to bolster cybersecurity, Reynolds said.

Lastly, to ensure local governments with less than 500,000 residents can access some of their state's CRF money for IT, good working relationships with state CIOs are essential, Reynolds said. "The challenge for those counties that did not get the money directly is how each state is administering that distribution," she said. "It's not necessarily a negative, but it does take more time to work through."

Step Three: Put the Funds to Work

In Montgomery County, Ohio, the Board of County Commissioners stood up the Office of CARES Act to manage and distribute $92 million in direct Federal funding under the CARES Act. Within each of the grant programs, the county is allowing technology expenses, and to date has obligated more than $1 million for IT-related expenses, said Michael Zimmerman, public information officer for Montgomery County Business Services.

"The need for technology services is huge right now," said Uchenna Youngblood, director of IT for the Montgomery County Board of County Commissioners. "We've focused on the actions we can take that best support Montgomery County citizens." Those efforts have included developing a grants management system, expanding Wi-Fi access to public parking lots, digitizing benefits applications, and enabling remote work with devices, collaboration platforms, and a redundant Internet connection.

San Antonio used a combination of CARES Act funds and city general funds to develop a social services case management tool and a COVID-19 online portal (https://covid19.sanantonio.gov/Home) for coronavirus information and recovery resources. It used CRF monies for other eligible uses in order to free $27 million in general funds to connect about 20,000 K-12 students to their respective school district's network from their homes, across 50 of the city's most vulnerable neighborhoods, CIO Craig Hopkins said.

To make critical investments quickly, "You need people who have different experiences, talents, and roles working together for a common cause – not just saying 'No' because they can only see what's in their silo," Hopkins said. In San Antonio, "It always starts with 'We're going to figure it out for our customers and our residents.' We just need to figure out what that looks like within the funding, the procurement rules, and our environment. We've got a great culture here that allows me to do that."

Step Four: Prepare for the Long Haul

Pandemic recovery is a marathon, public- and private-sector IT stakeholders acknowledged. The health crisis has exposed weaknesses and inequalities that the CARES Act and other funding programs are inadequate to address. Chief among them is broadband access for underserved populations – both rural and urban – to broaden access to telehealth, support distance education, and enable economic growth.

"We are very cognizant of competing priorities right now, but we hope state and local governments as well as Congress continue to focus on increasing access to broadband and high-speed Internet and 5G to bridge the digital divide," Griffin said.

State and local governments also need substantial funding for cybersecurity and IT modernization, Pincus and Reynolds observed. The State and Local IT Modernization and Cybersecurity Act (https://www.meritalk.com/articles/cyberspace-solarium-commissioners-intro-28b-bill-to-upgrade-slg-legacy-it/), introduced in mid-August in the House and Senate, calls for $28 billion in Federal funds to address COVID-19-related IT needs, modernize legacy IT infrastructure, and increase cybersecurity resiliency. "This would be huge for state and local IT because they wouldn't have to fight another agency" for funding, Pincus said. "I'm hopeful that at least some of it will get passed within the next year."

Recommendations From the Trenches

State and local government leaders – procurement teams, program managers, and IT executives who are in the trenches of pandemic response -- offer sage advice for securing and using CARES Act funds for IT initiatives:

Accomplish more by working together – elected officials, program leaders, procurement, and IT. The Summit County-Fairlawn court network partnership is one effort among longstanding collaborators. "Our philosophy is, 'We're only as healthy as our neighbors,'" said Fairlawn Mayor William Roth. "We all work together. Politics are really a non-issue."

Develop a robust governance process. In San Antonio, Hopkins is at the center of all IT spending. Several years ago, the city consolidated its IT operations into a single, shared service. Hopkins works with the deputy city manager and the chief financial officer to review and approve all technology investments. "I don't own all the money for technology, but I own all the approval of spend for it," he said. "My first job is to reuse what we have in our portfolio, and then to buy to fill a gap. I call it governance, but it's really just having a relationship with all the directors, understanding their needs, and applying what we have to their situation."

Document, document, document. "Make sure to tie spending to the criteria in place at the time of the spending," Shapiro advised. "We are trying to document everything so it's clear what we did and why we did it." For example, Fairlawn is documenting the time city staff spends on the FairlawnGig expansion to the courts. Those costs will be reimbursed from the $6.5 million in Summit County CARES Act funds allotted for the expansion.

Manage your timeline. "If I have a bucket of money that has a narrowly tailored usage, I can use it for that, and then create capacity elsewhere for other projects that are needed in the community," Bradshaw said. "It's really keeping the long game in mind, and not just racing to spend the money because of the timeline."

SHARE THIS STORY

TAGS: CARES ACT (HTTPS://WWW.MERITALKSLG.COM/TAG/CARES-ACT/)

How the shift to remote working has impacted cybersecurity

by **Lance Whitney** in **Security** on August 20, 2020, 8:19 AM PST

Cybercriminals have adapted by exploiting improperly secured VPNs, cloud-based services, and business email, says Malwarebytes.

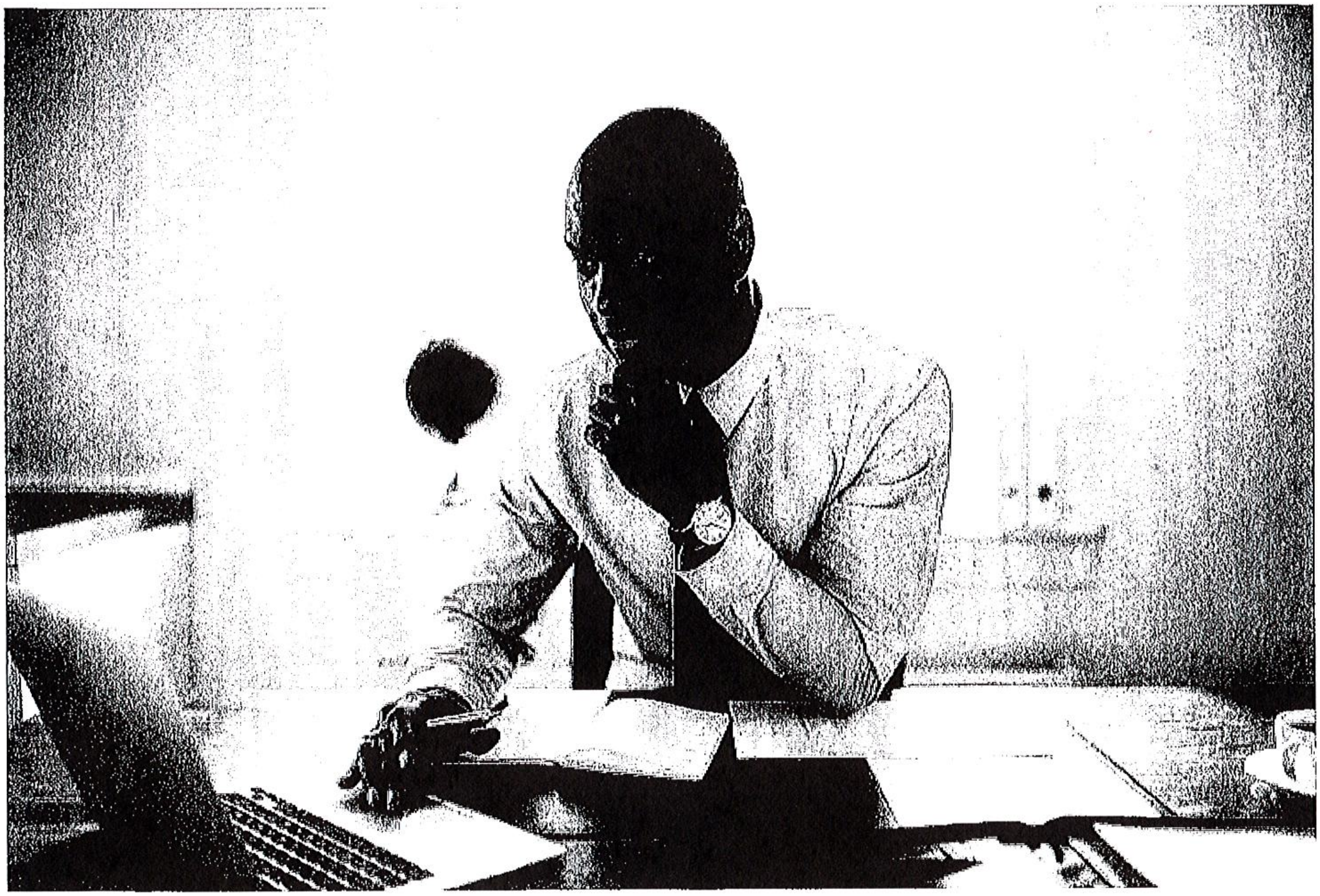


Image: Getty Images/iStockphoto

Triggered by the coronavirus lockdown, the abrupt transition to a work from home (WFH) venue forced organizations to scramble to support a larger remote workforce. Such a quick shift means that certain security measures and requirements inevitably fell by the wayside. At the same time, cybercriminals found a new opportunity for attack with remote workers and improperly secured connections and technologies. Together, these trends have created a more vulnerable environment affecting the cybersecurity defenses of many organizations.

SEE: Return to work: What the new normal will look like post-pandemic (free PDF) (https://www.techrepublic.com/resource-library/whitepapers/return-to-work-what-the-new-normal-will-look-like-post-pandemic-free-pdf/) **(TechRepublic)**

More about cybersecurity

- Top 5 programming languages for security admins to learn (https://www.techrepublic.com/article/top-5-programming-languages-for-security-admins-to-learn/)
- Top 10 antivirus software options for security-conscious users (https://www.techrepublic.com/article/top-10-antivirus-software-options-for-security-conscious-users/)
- Navigating data privacy (free PDF) (https://www.techrepublic.com/resource-library/whitepapers/navigating-data-privacy-free-pdf/)
- End user data backup policy (TechRepublic Premium) (https://www.techrepublic.com/resource-library/whitepapers/end-user-data-backup-policy-copy1-copy1/)

Released on Thursday by security firm Malwarebytes, a new report entitled "Enduring from home: COVID-19's impact on business security (https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf)" shines a light on how the transition has impacted security and how organizations can better handle the risks and vulnerabilities of working remotely.

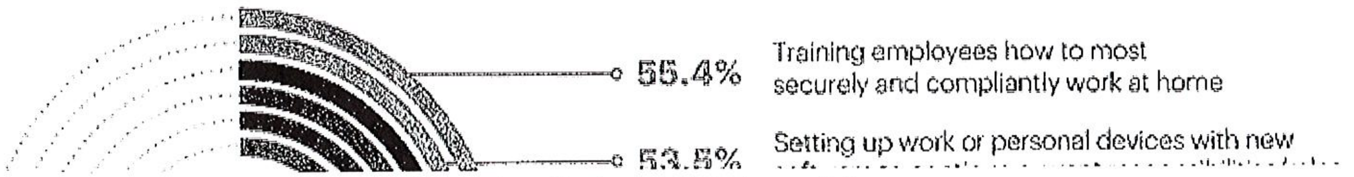
The report itself combines telemetry from Malwarebytes with survey results from IT and cybersecurity decision makers in the US.

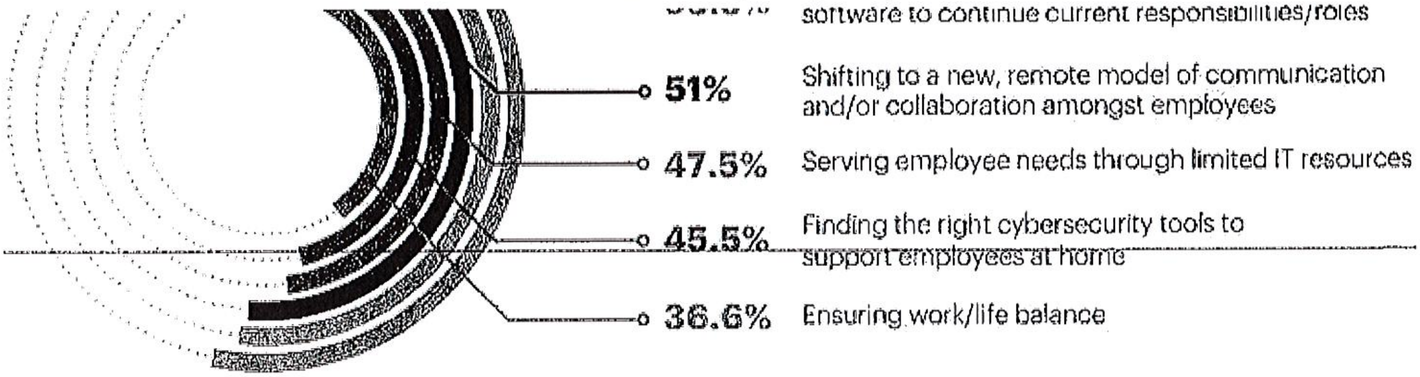
Due to the coronavirus lockdown, around one-third of the respondents had to shift anywhere from 81% to 100% of their employees to remote working. And more than two-thirds moved 61% or more of their workforce to a WFH mode. But most respondents felt their employer was prepared for the transition. Ranking preparedness on a scale of 1-10, with 1 being the least prepared and 10 being the most, the average ranking was 7.23. Only 14% of those surveyed ranked their company with a 4 or less.

However, organizations failed to address certain areas that would've strengthened security amid the WFH shift. Among those surveyed, 44% said they didn't provide cybersecurity training focused on the potential threats of working from home, 45% didn't analyze the security or privacy features in the software tools considered necessary for remote working, and 68% did not deploy a new antivirus solution for work-issued devices.

IT leaders also acknowledged a host of challenges in the move to working from home. A full 55% cited the need to train employees on how to securely and compliantly work at home as the top challenge. Some 53% mentioned the challenge of setting up work or personal devices with new software for employees to do their jobs remotely. And 51% pointed to the need to shift to a new, remote model of communication and/or collaboration among employees.

Organizations' biggest challenges to WFH





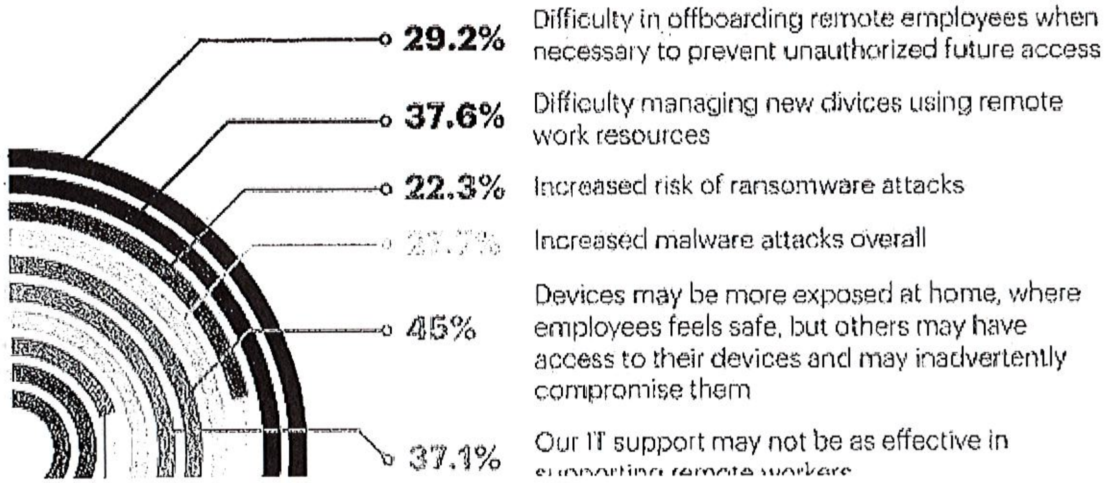
(https://tr2.cbsistatic.com/hub/i/r/2020/08/20/32276321-e45b-47c9-8037-bb87c8646746/resize/770x/eb5a3ea9a5cc7a2994157acb2a1fcc6e/wfh-challenges-malwarebytes.jpg)

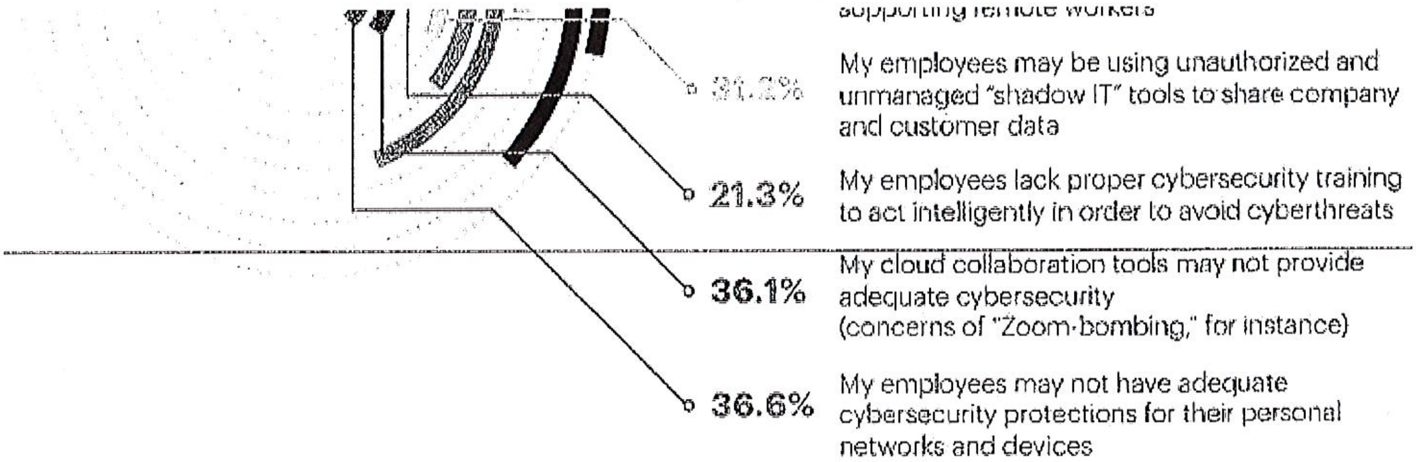
Image: Malwarebytes

Along with the challenges have come concerns due to the WFH transition. Among the respondents, 45% said their biggest concern was that devices may be more exposed at home where employees feel safe, but those devices could be accessed by other people who could accidentally compromise them. Several other concerns were cited by those surveyed, including the following:

- IT may not be as effective at supporting remote workers.
- Cloud collaboration tools may not provide adequate cybersecurity (concerns of Zoom bombing, for example)
- Employees may not have adequate cybersecurity protections for their personal networks and devices.
- Employees may be using unauthorized and unmanaged "shadow IT" tools to share company and customer data.
- Increased risk of ransomware attacks and malware attacks overall.

What are your biggest cybersecurity concerns with remote work?





(https://tr3.cbsistatic.com/hub/i/r/2020/08/20/05df8e58-afee-44d6-932a-96dd997322c9/resize/770x/bc801c004623ac147a86b2fd0e285472/wfh-concerns-malwarebytes.jpg)

Image: Malwarebytes

As a result of the shift to remote working, organizations have encountered a range of security issues. Among the respondents, 20% said they faced a security breach as a result of a remote worker. Some 24% had to spend money unexpectedly to resolve a security breach or malware attack following the WFH shift. Some 28% admitted that they're using personal devices for work more than their company devices, which could open the door for cyberattacks. And 18% acknowledged that cybersecurity was not a priority for employees.

"Many organizations failed to understand the gaps in their cybersecurity plans when transitioning to a remote workforce, experiencing a breach as a result," Malwarebytes CEO and co-founder Marcin Kleczynski said in a press release. "The use of more, often unauthorized, devices has exposed the critical need for not just a complete, layered security stack, but new policies to address work from home environments. Businesses have never been more at risk and hackers are taking notice."

What can and should organizations do to shore up their defenses while juggling the needs of a remote workforce? In its report, Malwarebytes offered a few suggestions based on the survey responses.

Develop stronger remote security policies. Cited by 55% of the respondents, stronger remote security policies are critical not just as a long-term strategy but as a way to unify cybersecurity defenses across the organization. The idea is to deploy remote work security guidance that views the organization from the standpoint of an attacker, which means being creative.

Install a permanent WFH model for employees who don't need to be in the office each day. Cited by 54% of those surveyed, this measure would help people who permanently work from home. But it would also benefit employees who need to access company resources when they're away on a trip.

Host more trainings for WFH. Cited by 49% of the respondents, training is important for employees working remotely. However, such training must be tailored to the needs and responsibilities of individual curity training will only help so much. Workers also are li ty advice is specific and relevant.

Develop online privacy revi hose surveyed said they plan to take this step to mak orkers function properly but also keep communicatio

Deploy antivirus solutions t **orce**. Cited by 44% of the respondents, this measure v eats targeting remote workers are older, commercial ones that could be detected by the proper security products.

Malwarebytes' survey received responses from 200 managers, directors, and C-suite executives in IT and cybersecurity roles at US companies. The survey included companies of different sizes, with some respondents working at small- and midsize businesses and others at large enterprises.

Also see

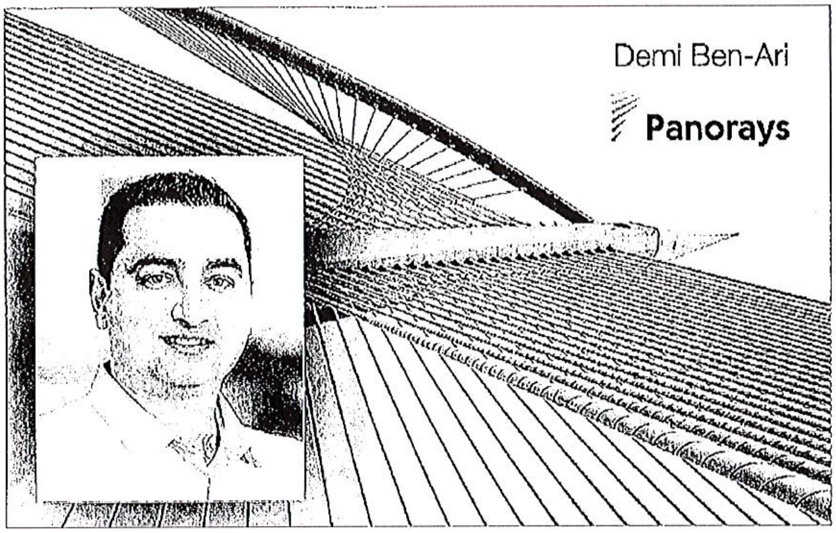
- Dark Web: A cheat sheet for professionals (https://www.techrepublic.com/article/dark-web-the-smart-persons-guide/) (TechRepublic)
- Video teleconferencing do's and don'ts (free PDF) (https://www.techrepublic.com/resource-library/whitepapers/video-teleconferencing-do-s-and-don-ts-free-pdf/) (TechRepublic)
- RFP templates and guidebook (https://www.techrepublic.com/resource-library/whitepapers/rfp-templates-and-guidebook/) (TechRepublic Premium)

Mirko Zorz, Editor in Chief, Help Net Security
March 20, 2020

Share f in

The cybersecurity implications of working remotely

We sat down with Demi Ben-Ari, CTO at Panorays, to discuss the cybersecurity risks of remote work facilitated by virtual environments.



The global spread of the COVID-19 coronavirus has had a notable impact on workplaces worldwide, and many organizations are encouraging employees to work from home. What are the cybersecurity implications of this shift?

Having a sizable amount of employees suddenly working remotely can be a major change for organizations and presents numerous problems with regard to cybersecurity.

One issue involves a lack of authentication and authorization. Because people are not seeing each other face-to-face, there is an increased need for two-factor authentication, monitoring access controls and creating strong passwords. There's also a risk of increased attacks like phishing and malware, especially since employees will now likely receive an unprecedented amount of emails and online requests.

Moreover, remote working can effectively widen an organization's attack surface. This is because employees who use their own devices for work can introduce new platforms and operating systems that require their own dedicated support and security. With so many devices being used, it's likely that at least some will fall through the security cracks.

Finally, these same security considerations apply to an organization's supply chain. This can be challenging, because often smaller companies lack the necessary know-how and human resources to implement necessary security measures. Hackers are aware of this and can start targeting third-party suppliers with the goal of penetrating upstream partners.

What are the hidden implications of human error?

With less effective communication, organizations are unquestionably more prone to human error. When you're not sitting next to the person you work with, the chances of making configuration mistakes that will expose security gaps are much higher. These cyber gaps can then be exploited by malicious actors.

5 tips to reduce the risk of email impersonation attacks

Data protection predictions for 2021

Moving to the cloud with a security-first, zero trust approach

Webinar: How to think about cybersecurity the way executives think about business

What's new

DNS attacks increasingly target service providers

Attackers finding new ways to exploit and bypass Office 365 defenses

HITBSecTrain: Cutting-edge virtual cyber security trainings on a monthly basis

Hackers breach psychotherapy center, use stolen health data to blackmail patients

IT departments are especially prone to error because they are changing routine and must open internal systems to do external work. For example, because of the shift to a remote workplace, IT teams may have to introduce network and VPN configurations, new devices, ports and IT addresses. Such changes effectively result in a larger attack surface and create the possibility that something may be set up incorrectly when implementing these changes.

The fact that people are not working face-to-face exacerbates the situation: Because it's harder to confirm someone's identity, there's more room for error.

What are the potential compliance implications of this huge increase in mobile working?

There's greater risk, because employees are not on the organization's network and the organization is not fully in control of their devices. Essentially, the organization has lost the security of being in a physical protected area. As a result, organizations also open themselves up to greater risk of not adequately complying with regulations that demand a certain level of cybersecurity.

Another compliance issue is related to change. For example, an organization may be certified for SOC2, but those controls may not remain in place with people working from home. Thus a major, sudden change like a mass remote workforce can unintentionally lead to noncompliance.

How can organizations efficiently evaluate new vendors, eliminate security gaps and continuously monitor their cyber posture?

As part of their third-party security strategy, organizations should take the following steps:

1. Map all vendors along with their relationship to the organization, including the type of data they access and process. For example, some vendors store and process sensitive data, while others might have access to update software code on the production environment.

2. Prioritize vendors' criticality. Some vendors are considered more critical than others in terms of the business impact they pose, the technology relationship with an organization or even regulatory aspects. For example, a certain supplier might be processing all employee financial information while another supplier might be a graphic designer agency that runs posters of a marketing event.

3. Gain visibility and control over vendors. This can be accomplished by using a solution to thoroughly assess vendors, preferably with a combination of scanning the vendor's attack service along with completion of security questionnaires. With the shift to remote working, organizations should also be sure to include questions that assess vendors' preparedness for working at home.

4. Continuously monitor vendors' security posture. Visibility and control require a scalable solution for the hundreds or even thousands of suppliers that organizations typically engage with these days. Organizations should ensure that their solution alerts of any changes in cyber posture and that they respond accordingly. For example, organizations may decide to limit access, or even completely close connections between the supplier and the organization's environment.

More about

CISO coronavirus cybersecurity human error mobile devices mobile security opinion

Panorays remote working strategy supply chain tips

Share this

Featured
news

Hackers breach psychotherapy center, use stolen health data to blackmail patients

Attackers finding new ways to exploit and bypass Office 365 defenses