Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Practical advice for compliance:

TACKLING CORONAVIRUS RISK

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

Inside this e-Book

Pandemic, gov't money: Perfect storm for fraud

A global pandemic, an unprecedented flow of government money, and a weakening of lending controls could create a perfect storm of opportunity for fraudsters, writes **Aaron Nicodemus**.

The United States may be entering a golden age for financial fraud.

A global health pandemic, an unprecedented flow of government money, and a weakening of lending controls and oversight could create a perfect storm of opportunity for individual fraudsters, criminal gangs, and even enemies abroad to lay their hands on $2 trillion in taxpayer dollars meant to support the American economy, financial crimes experts say.

"There is potential for a significant amount of fraud. We're potentially talking tens or hundreds of billions of dollars here," said Daniel Wager, vice president of global financial crime compliance for LexisNexis Risk Solutions and a former federal investigator and bank executive.

Brandon Daniels, president of global markets with Exiger, a GRC consultant firm, agreed. "There are several angles through which risk is escalating," he said. "There is a huge amount of money being pushed out to support small businesses, which would help the U.S. population live day-to-day. And there is a huge volume of criminals looking to siphon away funds from the regulated financial system."

This perfect storm starts with opportunity, in the form of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). The CARES Act authorizes $2 trillion in relief to American businesses and industries, including $454 billion in Federal Reserve lending power. President Donald Trump and Congress want to push that money out to American taxpayers and businesses as soon as possible; checks began flowing to individual taxpayers in April.

There are troubling signs that oversight of the CARES Act may not even be as robust as the oversight of the last significant relief package, the Emergency Economic Stabilization Act of 2008.

The Emergency Economic Stabilization Act of 2008 —which authorized the Treasury Secretary to create the $700 billion Troubled Asset Relief Program (TARP)—and the $840 billion stimulus package under the American Recovery and Reinvestment Act of 2009, was roughly combined at $1.5 trillion.

Oversight of the TARP funds fell to the Office of the Special Inspector General for the Troubled Assets Relief Program (SIGTARP). The agency has recovered $11 billion and convicted over 380 people in financial fraud investigations since it was launched, according to a 2019 press release. SIGTARP eventually moved beyond simply clawing back money from TARP and is conducting independent financial crime investiga-

tions. It also established a Financial Fraud Registry as a place to highlight and coordinate financial fraud investigations conducted by various federal agencies.

The CARES Act creates a similar oversight body, the Office of the Special Inspector General for Pandemic Recovery (SIGPR). However, there have been several troubling signs its investigatory strength may be hamstrung or curtailed. President Trump in his signing statement accompanying the CARES Act relayed his intent not to enforce the oversight provision, arguing that it interferes with executive branch prerogatives. "My administration will treat this provision as hortatory but not mandatory," he wrote.

Since then, President Trump took an additional step to rein in the potential investigatory strength of SIGPR. He removed acting Inspector General Glenn Fine, an experienced independent investigator who had worked in the Pentagon since 2016. Fine was poised to provide independent oversight on the $2 trillion CARES Act spending as head of SIGPR. The president appointed in his place Environmental Protection Agency inspector general Sean O'Donnell, who was appointed to the EPA in January.

"If we use past historical models as a guide—Katrina, Hurricane Sandy, other natural disasters—we can expect double digit (percentage of) fraud here," Wager said. The difference, he said, is the scale. The CARES aid package is massive, and politicians want the money pushed fast. "It's a factor being weighed politically right now, how much fraud is too much," he said. "All indications are the government is distributing money with an eye towards generosity, and not the same eye towards reclamation and recovery."

Financial institutions are under increasing pressure to approve government loans quickly. Some of that pressure has been relieved by recent announcements by two federal agencies, indicating they will loosen certain loan verification and reporting requirements under the Bank Secrecy Act. The government will still expect banks and lending institutions to do their due diligence, Wager said. But they will have to find ways to speed up the vetting process.

"In the past, this process was done manually, so they need to find ways to process loans in batches, en masse," he said. Many of the red flags that might normally pop up—say, a business has no revenue for an entire month or has produced no invoices—should be overlooked, he said, because a borrower's slowing or stopping of business activity is the new normal.

One of the ways financial institutions can do this is by repurposing software that had been used by financial institutions to vet companies and individuals seeking loans, a process that was usually driven by analysts, Daniels said.

Now, that same software can be used by government to flag companies that have recently switched from manufacturing one product to another. Companies that have recently jumped into the medical supply or toilet paper business probably need more scrutiny. A company that had never sold medical supplies before suddenly jumping into the market could be a red flag, he said.

But even that vetting has its pitfalls, because some manufacturers are reopening parts of their shuttered lines to produce personal protection equipment like masks, or key medical supplies like ventilators, then donating the products to front-line medical workers.

In lieu of some of these more traditional forms of vetting a business, Daniels says some financial institutions are examining supply chains. For example, a company that manufacturers window seals may be competing for a key ingredient with manufacturers of badly needed medical supplies. The window seal manufacturer is going to have trouble sourcing that ingredient in the short term.

That doesn't mean the window seal manufacturer doesn't get a loan, but it could affect the type of loan, Daniels said. They'd be more suited for a straight relief loan, rather than a loan that helps them compete for a government contract, for example.

For all this talk about fraud, maybe some fraud isn't a bad thing, or at least tolerable, in this current environment, Wager said. "Fraudsters tend not to save. They're great spenders," he said, laughing. "They love buying cars, boats, going on fancy vacations. We always have the chance to pursue fraud in arrears." ■

Do we compromise privacy to be safe from coronavirus?

How much of your privacy rights are you willing to give up in the fight against the coronavirus pandemic? The answer might determine how successful we are in the next phase. **Aaron Nicodemus** explores.

How much of our privacy rights and civil liberties will we be willing to give up in the fight against the coronavirus pandemic? After the terrorist attacks of Sept. 11, 2001, Americans showed they were willing to allow these basic rights to erode—a little here, a little there—in exchange for safety.

The coronavirus is an even more insidious threat than terrorism. It has no agenda, respects no borders, and preys on the old and the sick. Successfully beating back this virus may require further erosion of these basic rights in a democracy. But this time, working hand-in-hand with government to monitor our behaviors and restrict our movements, could be some of America's biggest companies.

How will it happen? Let's examine the pandemic response playbook. The playbook's first two responses to an infectious disease outbreak are identification (testing), then isolation. North America and Europe are still mostly still tackling these two responses.

Contact tracing, the third response, has been mostly forced to the sideline as hospitals overflow with desperately sick patients and healthcare workers struggle to obtain sufficient personal protective equipment. But contact tracing may come to dominate the response to the pandemic this summer.

What's contact tracing? Once a person has tested positive for coronavirus and has been isolated, health officials attempt to establish every person the infected patient came into close contact with in the past two weeks. Then they contact those people and advise them to watch for symptoms as they self-isolate.

Contact tracing has been used successfully in China and South Korea to limit the spread of coronavirus. Several U.S. states, including Massachusetts, are examining how to ramp up contact tracing this summer while hiring lots of people to conduct it, according to STAT, a healthcare industry reporting Website.

We probably have to accept contact tracing as a necessary evil. It will help to slow coronavirus hotspots and to beat back a potential second wave of infections.

For contact tracing to work, we in democratic, western societies will have to give up a little bit of our rights. Remember what it was like to travel before 9/11, then after? Remember our tolerance for government eavesdropping before, and after? For torturing terrorism suspects before, and after? Like that.

This time, though, we may be ceding our rights to Big Tech. Google and Apple recently announced a partnership that will call a truce between these fierce corporate rivals in the name of fighting coronavirus. The firms will allow their current Android and iOS devices to interface with each other "using apps from public health authorities" for the purpose of using their devices to trace who they've been in contact with.

While the tech giants expect to release their portion of the technology in May, it will likely be into the summer before public health authorities release a contact tracing app to the public.

Here's how it would work. People would voluntarily download the app, and it would begin collecting information on their movements, stored only on their mobile devices. If the person tests positive for coronavirus, s/he would enter that information into the app.

The app would then notify all people whose smart phones (with the voluntary app) have been within six feet of the infected person in the past two weeks. Those people would be advised to self-isolate for two weeks. Some privacy experts worry that the technology is ripe for misuse, either by government, Big Tech, or other bad actors.

"Contact tracing apps collect and combine two highly sensitive categories of information: location and health status," wrote University of Washington Law Professor Ryan Calo, in April 9 testimony before the U.S. Senate Committee on Commerce, Science, and Transportation. "It seems fair to wonder whether these apps, developed by small teams, will be able to keep such sensitive information private and secure."

He went on to list other concerns, like that the app would be inaccessible to the poor, that it could show an area as "safe" only because few users had downloaded the app, or how people could game the system by uploading fake positive tests to make an area look like a hotspot.

This entire argument also depends on the government ramping up coronavirus testing so that everyone—not just those showing symptoms, because health officials acknowledge that 25-50 percent of people infected may show only mild symptoms—can be tested. At least in the United States, we are far, far away from universally available coronavirus tests.

Back to the privacy and civil liberty concerns. Google and Apple have pledged to be as open and transparent as possible, while also protecting the privacy of people using the app. "Privacy, transparency, and consent are of utmost importance in this effort, and we look forward to building this functionality in consultation with interested stakeholders," the companies said in their statements. "We will openly publish information about our work for others to analyze."

The Trump regime has not yet unveiled how much information it intends to reveal about the creation and use of this app, and that has some Democrats worried. "I would hope that the Department of Health and Human Services—and the Trump Administration as a whole—follow similar steps to be more transparent and, for example, publish the full agreements they have signed with tech companies such as Apple," U.S. Sen. Robert Menendez (D-N.J.) told The Verge.

The Trump administration hasn't said if it will release those agreements, or much information at all at this point. It will be up to us—the people who will be subject to contact tracing and who voluntarily agree to use this technology to track our movements—to demand that the Trump administration make this information available.

We should demand to know the terms of the deal the government is making with these companies in order to create this app. We should demand to know how it is protecting our rights under the Constitution. And we should know how the government will ensure the data collected will not be used for purposes other than contact tracing.

Americans may very well be willing to give up a little bit of privacy, a little bit of control, in order to be made safer. We just want to know if it's worth it. ■

Navigating the return of employees to the workplace

Aaron Nicodemus has more on the ethical and legal quandaries employers will be facing when they get the go-ahead from healthcare experts and state and local officials to bring employees back into the workplace.

Bringing employees back from working from home means reacting to ever-changing recommendations from health experts as well as the mandates of state and local officials.

The last thing any employer wants to do is start a new coronavirus hot spot in the workplace.

With many parts of the United States and Europe still under stay-at-home orders, the idea of returning workers to the workplace may seem like a faraway dream. The process will likely be uneven and frustrating, full of starts and stops.

When workplaces reopen, employers will have to navigate a number of legal and ethical quandaries, employment attorneys say. That's especially true for employees who tested positive for coronavirus or who experienced symptoms of the infection but weren't tested.

"It used to be that you needed a note from your doctor to return to work. Employers could hang their hat on that," said Mark Neuberger, an employment attorney at the firm Foley & Lardner. "In this crazy environment, it's tough to get a doctor to sign off."

Employers still have the right to tell an employee it's too soon to return to work.

"I think employers have to be overly cautious," he said.

So are there any screenings worth considering?

The most common and easiest to implement would be to require all returning employees to submit to a touchless temperature screening before being allowed to enter the workplace.

"Before the pandemic, most people would have found this ridiculous and it could have spurred a lawsuit," Kwabena Appenteng, a shareholder in Littler Mendelson's Workplace Privacy and Data Security Practice Group, said of screening employees for fevers. "Now, it's recommended by the CDC (Centers for Disease Control and Prevention) and numerous states and counties, and many of our clients have instituted this screening method."

Even then, taking temperatures might not catch all infections. One-fourth of people infected with coronavirus might not express symptoms like a temperature, CDC Director Robert Redfield said in an interview.

Pre-pandemic, the U.S. Equal Employment Opportunity Commission (EEOC) considered taking a temperature a medical procedure, which could violate the Americans with Disabilities Act. Asking medical questions could also constitute a violation, the EEOC said.

But the EEOC has since loosened its recommendations on temperature checks and medical questions during a pandemic, according to a March 18 bulletin. During a pandemic, it is permissible to take an employee's temperature and to ask employees whether they are experiencing any of the symptoms of a coronavirus infection, such as "fever, chills, cough, shortness of breath, or sore throat."

According to experts, those recommendations, however, could change.

"Employers should remember that guidance from public health authorities is likely to change as the COVID-19 pandemic evolves. Therefore, employers should continue to follow the most current information on maintaining workplace safety," the EEOC said.

"It used to be that you needed a note from your doctor to return to work. Employers could hang their hat on that. In this crazy environment, it's tough to get a doctor to sign off."

Mark Neuberger, Employment Attorney, Foley & Lardner

Other employers are considering screening for coronavirus antibodies in an employee's blood. Health experts have not yet studied antibodies long enough to know if having them shields a person from reinfection, however.

Appenteng says employers would do well to consider how long they intend to implement coronavirus screening protocols like temperature checks, health questions, or blood testing, given that not all protocols will remain permissible as the pandemic subsides.

"That might drive what you choose," he said.

Employers should also be wary of discrimination against sick employees who return to work.

According to a recent coronavirus workplace survey of over 900 employers by the employment law firm Littler Mendelson, "most respondents were extremely to moderately concerned (44 percent) or somewhat to slightly concerned (39 percent) about unintentionally discriminating against members of a protected class or giving rise to discrimination claims. However, this issue ranked lowest in the list of concerns posed to respondents and 17 percent indicated not being concerned at all, suggesting that this is an area that employers should continue to be mindful of in this rapidly evolving situation."

To help avoid discrimination, employers should only collect the minimal amount of health data necessary to allow an employee to return to work, said Hilary Wandall, senior vice president, privacy intelligence and general counsel at TrustArc, a compliance and risk management consulting company. That data should be shared only with other employees who need to know and should be stored in a place that is separate from company data that is accessible to other employees.

"It's very important for compliance officers to think about privacy obligations," she said. "You want to be transparent about the processes" but not inadvertently share private employee health data with other employees, she said.

Some industries are learning on the fly

Sections of the retail industry—supermarkets, pharmacies, liquor stores, and some department stores—that have remained open throughout the pandemic may offer cautionary tales.

The family of a Walmart employee killed by coronavirus in Illinois sued the retail giant, claiming the company did not do enough at his workplace to shield him from contracting the virus.

The United Food and Commercial Workers International Union, which represents over 900,000 grocery workers, announced in mid-April that 30 union members had been killed by coronavirus and nearly 3,000 had been infected.

"Since the beginning of the outbreak, these workers have been on the front lines of this terrible pandemic, said United Food and Commercial Workers President Marc Perrone in a statement. "While tens of millions of Americans were told to work from home for their safety, grocery store and food workers have never had that option."

By mid-April, Stop & Shop, a 400-store supermarket chain stretching from Maine to New Jersey owned by Dutch conglomerate Ahold Delhaize, had at least four employees test positive for coronavirus, according to a Channel 10 (Rhode Island) news story. The company did not return a request for comment.

Jim Carvalho is the business agent and political director for UFCW Local 1445 in Dedham, Mass., which represents approximately 10,000 Stop & Shop workers in Massachusetts.

Carvalho said Stop & Shop offers two weeks of paid leave to employees who are out of work due to coronavirus. Management stays in contact with the employee's doctor during the leave, he said. There are no screenings for employees who have recovered and can return to work, Carvalho said. ■

Amii Barnard-Bahn
CW Columnist

Ask Amii mailbag

Amii Barnard-Bahn addresses tackling the unchartered territory of the coronavirus pandemic.

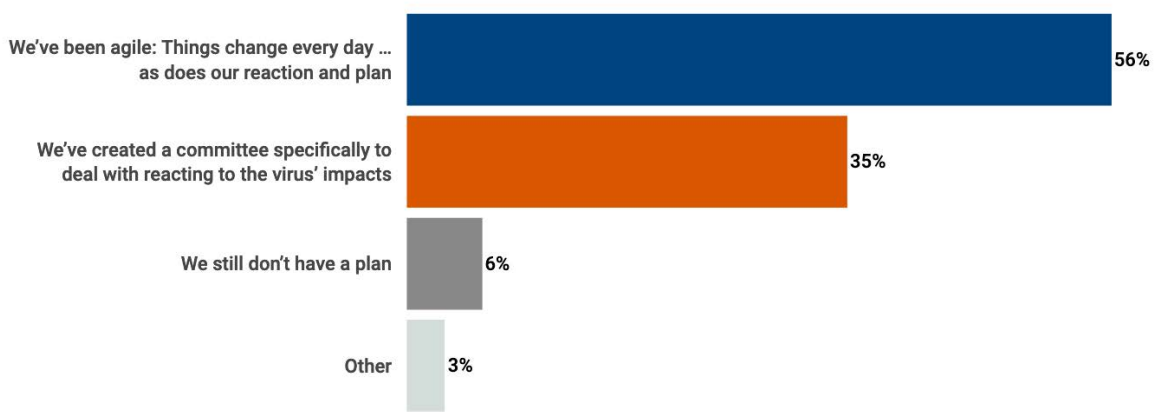
How prepared can you be for the unknown?

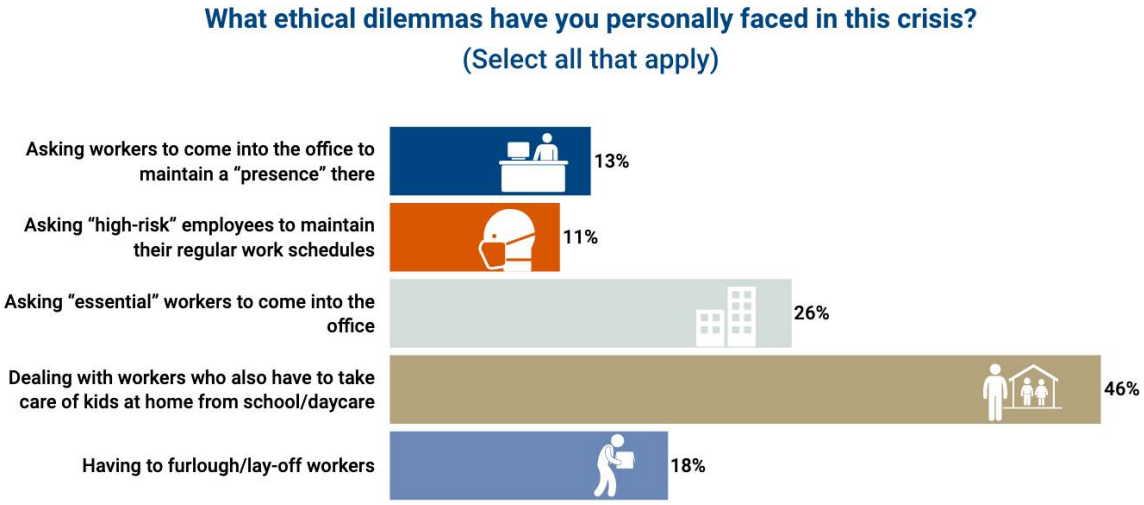
Q: Like many companies, we are in unprecedented territory with this coronavirus. We're taking things day by day, piecing together plans as we go. I feel like we need to have some sort of committee that meets daily to discuss this. Do you know of companies that have gone that route? Is there a "best practices" for dealing with a crisis like this one?

Amii: A crisis committee is certainly a best practice for fast-moving crises like COVID-19. Based on Compliance Week's survey released in late March, 1/3 of respondents have put a committee in place. Another 56 percent acknowledge that their plan and response to the pandemic changes every day.

Everyone should have a crisis plan that can be applied to various risk scenarios. Key members usually include employee communications, IT, HR, public relations, and legal. Have alias lists (an e-mail list for a group, such as "crisis committee," "executive management," or employees in specified geographic locations) and chain-of-command checklists about

What steps has your company taken to create (or update) its pandemic preparedness plan since the coronavirus pandemic began?





what information needs to go out to who (e.g. customers, strategic partners). Having a pre-identified team enables you to quickly jump into action so that when a crisis does arise, you have the basics and can start having regular meetings to take action on any special circumstances like having to shift to a work-from-home mode of business.

Whatever the crisis, you will need to make a business operation shift away from standard operating protocols and effectively communicate these changes through various channels. For example, your customer marketing may need to shift from a "sell" mode to one of empathy and compassion—or you risk being tone-deaf to what is happening in the world and alienating customers. If you don't have a plan in place, make sure you document everything you are doing as you go through it now so that when a similar situation arises (such as a second pandemic wave) you can leverage your previous work.

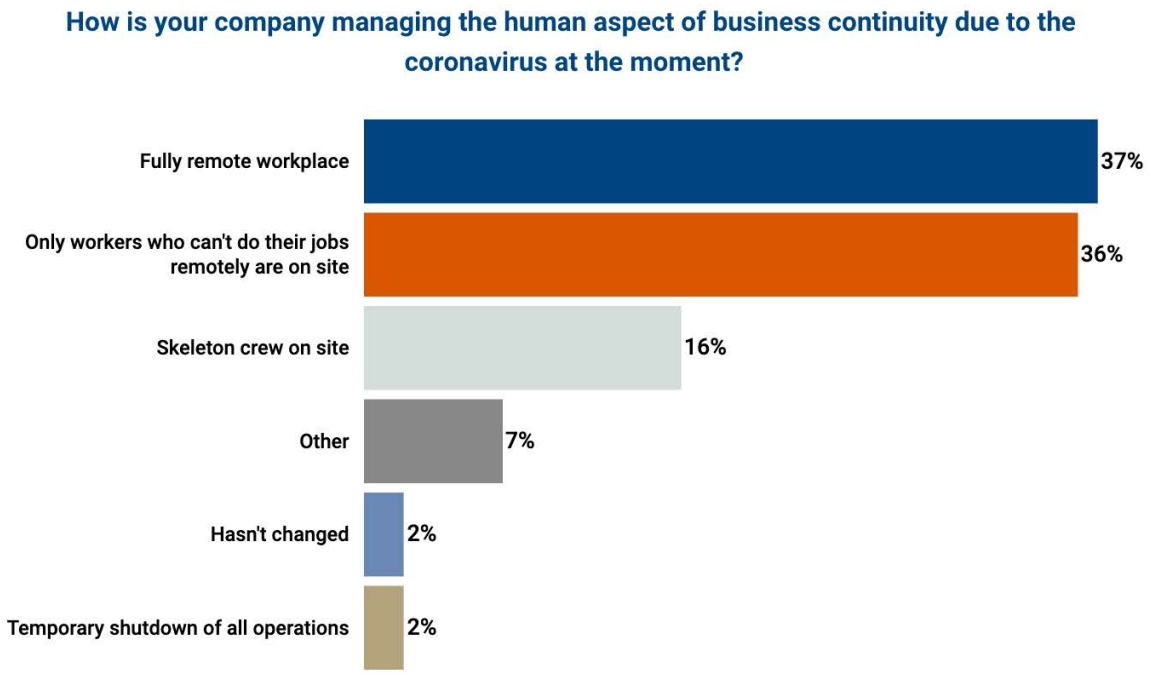
Q: Our CEO insists on having "a presence" in the office each day (we're in Chicago) during this pandemic, to pick up the mail, maintain some semblance of continuity I guess. We're a small company (75 employees) and, realistically, we can all do our jobs from home. Behind the scenes I am pushing for that, but our CEO maintains we need to have a skeleton crew in each day to keep continuity. I argue we are putting employees in danger. What's "the right thing to do" here?

Amii: You are right to be concerned and wise to be questioning your CEO's approach. This is an unprecedented time for our generation of leaders, and requiring employees to work in the office when they can perform their work remotely exposes people to an unnecessary health risk. In CW's survey, asking employees to come into the office just to maintain a "presence" was cited as a personal ethical dilemma currently faced by 13 percent of C&E professionals.

Based on the survey, as of March 31, 37 percent of respondents were fully remote and another 36 percent of responding companies were only allowing in-person work that could not be performed at home. If it's any indication, all of my client companies have closed their offices and are remote at this time.

For guidance, you can look to national, state, and local government mandates to determine those that apply to your company. Your PR or Public Affairs team may pull together a daily news clips summary on a crisis to send to your management team to keep them informed on the latest and the measures that your industry and competitors are taking. Seeing what other leaders/companies are doing may help them make better informed decisions.

My personal opinion: If you can run your business effectively without any employees in the office, I would strongly urge your CEO to do so. When we recover from this crisis, employees will remember and eval-



uate how and whether their company demonstrated care and concern for their well-being—and failure to do so will negatively impact employee engagement and retention for the long-term. As stated by Mark Cuban recently on CNBC, how employers handle this will "define their brand for decades."

Q: Should companies have had a "pandemic" plan in place? We made a lot of contingency plans in place (terrorist attack, major fire at our facility, etc.), but nothing for pandemic. We ended up adapting some parts of our other plans on the fly. Do you think we're alone in not having that kind of plan in place? Right now we're already having meetings about the "second wave" (very depressing).

Amii: While rare, the impact of a pandemic or biological threat is so great that in 2016, the U.S. National Security Council created what became informally known as the "pandemic playbook" (officially titled, "The Playbook for Early Response to High-Consequence Emerging Infectious Disease Threats and Biological Incidents"). The playbook was created in response to an inadequate global leadership response during the 2014-2015 spread of Ebola.

Know you are not alone—many companies did not have a plan in place to meet the demands of this crisis. Based on the CW survey, a slight majority (56 percent) of respondents had a plan, while 44 percent did not. And, like you, 76 percent of companies are preparing for a potential second COVID-19 wave, taking actions such as refining their response plan, assembling a crisis team, communication plan, facilitating virtual work-from-home, and cross-training employees. Based on current medical knowledge and predictions, it's wise to be prepared for the possibility of a second wave. ■