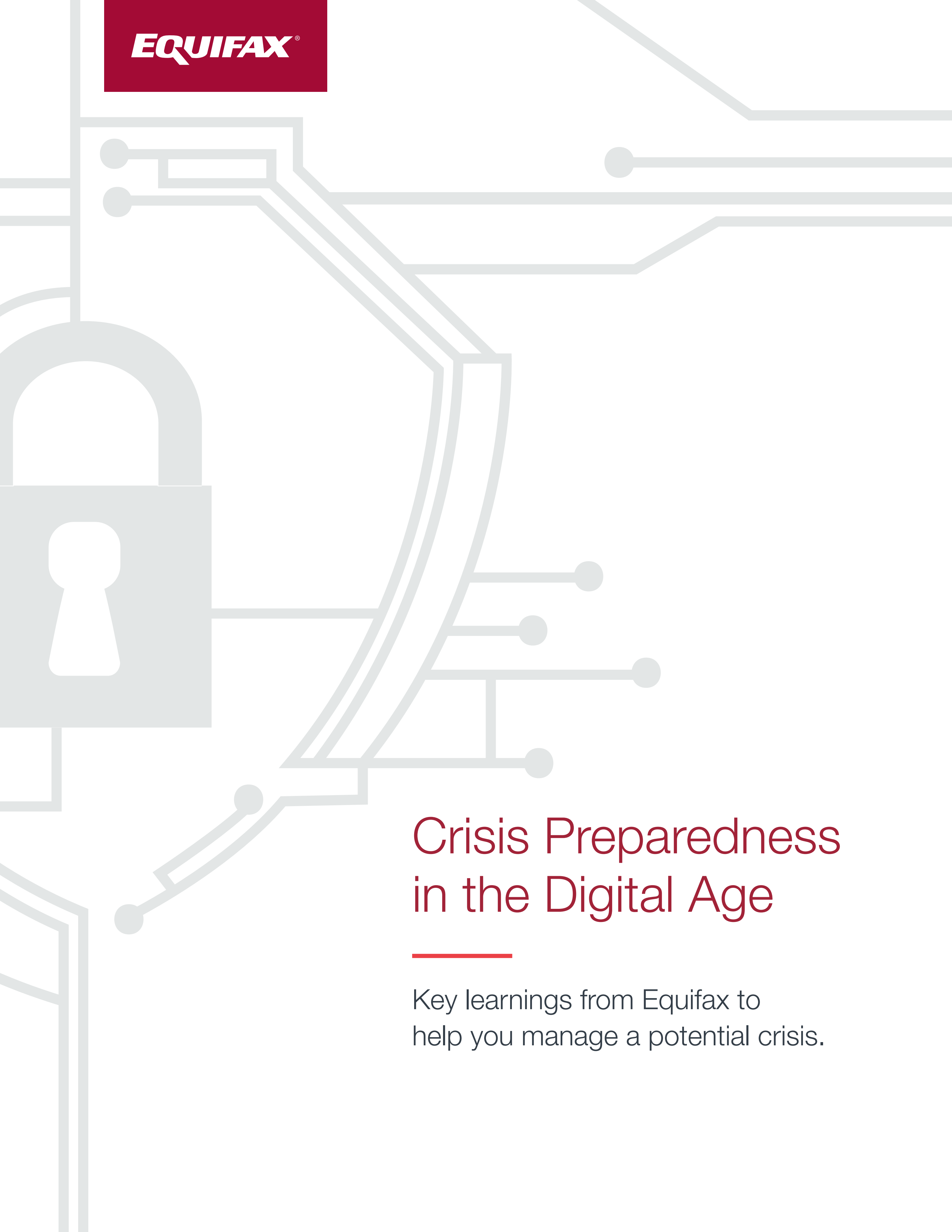
EQUIFAX®



Crisis Preparedness in the Digital Age

Key learnings from Equifax to help you manage a potential crisis.

If your organization is like many, you may think you're equipped to manage something like a major cybersecurity incident. The reality, however, is that you're probably not as ready as you think. Given the fast-changing nature of cyber and other types of risk, there is now more to be aware of and prepare to do if you experience such an event.

It is almost impossible to be fully prepared for a large-scale crisis. But most organizations can nonetheless take steps to be better prepared to manage one.

In today's digital world, news spreads more quickly than ever, fueled by a new media landscape driven by clicks and shares. At the same time, business crises are on the rise, with data breaches joining product recalls, workplace equity and natural disasters in the ranks of incidents that demand a coordinated crisis response. In 2017, the Institute for Crisis Management (ICM) tracked more than 800,000 crisis news stories, up 25 percent over the year before.[1] Yet just over half of all organizations have a crisis plan in place, according to ICM.

It is almost impossible to be fully prepared for a large-scale crisis, but most organizations can be better prepared to manage one. Preparedness for a cyber incident goes far beyond the purview of the chief information security officer (CISO) or risk management function—it needs to be on the entire C suite's agenda, regardless of industry or the size of the organization. The same holds true for other workplace issues—embedding and implementing systems to address and manage reports of potentially inappropriate workplace behavior, for example, isn't just HR's responsibility.

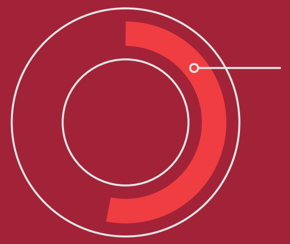
At Equifax, we were hit by a major cyberattack in 2017, and we have since undergone some fundamental shifts in how we do business as a result. While we did a lot to prepare for such an event, we learned a lot from the experience as well. From crisis management to external support and communications, we've gleaned key insights that are helping guide our ongoing evolution.

If there's any silver lining in our situation, it's that we've had a tremendous opportunity to reflect, adjust and make changes, and we feel a responsibility to share what we've learned along the way. By talking openly about our key learnings and providing some actionable things your team can practice or implement, our hope is that we can enable you to effect change within your organization or at the very least open a dialogue about how prepared you really are for a crisis.

Crisis Management

Eighty percent of organizations worldwide have had to mobilize their crisis management teams at least once in the past two years,[2] but organizations' confidence often exceeds their crisis-response preparedness.

And it's impossible to foresee every possibility. Organizations often plan for things like hurricanes, power outages or a cyberattack, but consider asking yourself one additional question: What would your worst enemy do if it wanted to put you out of business?



Just over half

of all organizations have a crisis plan in place, according to the Institute for Crisis Management (ICM).

How to Prepare:

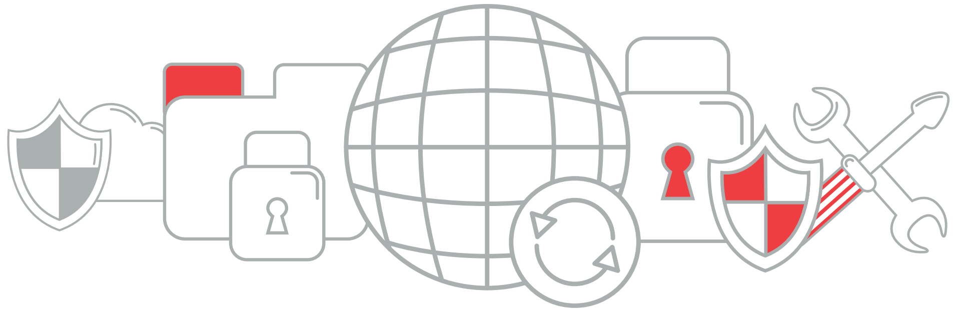
When stress-testing your organization's preparedness, identify the worst-case scenario, then practice your response over and over again. It's also a good idea to stress-test your approval and decision-making processes. If you don't practice them, you won't know with certainty whether they work.

You also need to have one decision-maker everyone agrees upon in advance. This person can, of course, seek counsel and advice, but the responsibility for making decisions and continuing to move forward lies with him or her. Nearly 85 percent of U.S. employees work in a matrixed organization,[3] but when the stakes are high and time is short, the matrix has to go out the window.

To respond quickly and effectively, your crisis plan should be simple, realistic and actionable. By focusing on a few key things, you can execute those things well. But don't forget to document the details you will want to remember while the crisis is unfolding—pulling advertisements or turning off marketing posts, for example. This preparation will free your teams to focus on the immediate need—your crisis response.

Lastly, establish a culture of accountability and risk-based decision-making. To reinforce this culture at Equifax, we changed our structure so that our CISO reports directly to the CEO and has a seat at the table for all business decisions. This change reflects the increasingly important role of the CISO in the digital age, in which data breaches are increasing in number and magnitude across the board. It also helps ensure that security and risk are considerations in everything from mergers and acquisitions to product launches.

A key part of a healthy culture is aligning behaviors and mindsets to a common purpose—and establishing metrics in support of that purpose. This can include tying incentive compensation to the company's security goal, as we have at Equifax. These types of actions can help set cultural norms and expectations throughout the organization.



External Support

When facing a crisis, the C suite can't do it alone—you will probably need specialized expertise and some extra hands—think law firms, communications consultants, forensic experts and operations support.

Identify all external support resources needed ahead of time—critical vendors, suppliers, consulting firms, operations support, etc.—and include them in your simulations and stress tests.

How to Prepare:

Act now to select the individuals or firms that will serve as your support and put processes in place to be able to onboard them quickly. To avoid delays, have the key provisions of your contracts negotiated and think about other logistics that you can arrange in advance, such as entering vendors into systems so that they can begin working immediately when a crisis hits.

Knowing your vendors and suppliers ahead of time will come in handy when evaluating the capacity of your IT infrastructure, and your ability to exponentially increase it in short order, for any customer or consumer operational support centers. You may need to prepare for a higher volume of calls across geographies and customer contact channels and in multiple languages. Have a back-up plan for the back-up plan to help you address the inevitable surprises that pop up.

Communications

Contrary to the common idiom, you should definitely sweat the small stuff. Communication is one of the most important elements of a crisis response, and with today's fast-moving 24/7 news cycle and variables out of your control, it can be the most challenging. News moves at lightning speed, and if you do not respond quickly, you may miss your opportunity to respond at all. It isn't uncommon for a reporter to call with a question and give your organization 20 minutes to respond. Those requests rarely tie in nicely with the playbooks and pre-approved statements you assembled so carefully in advance, leaving you scrambling to come up with a response.

> "Communications is absolutely the hardest part of managing a crisis—**by a factor of 10.**"

How to Prepare:

When you're under scrutiny, as is often the case in a crisis, responding accurately and as completely as possible is important. Any missteps you make in your response are amplified. A single reporter's story can be picked up by dozens of other outlets, which means that any inaccuracies or misperceptions can spread widely. It's often a delicate balance—you need to be as transparent as possible while ensuring that your communications are accurate and supported by facts. You want to be able to make clear, definitive statements, but there aren't always clear, definitive answers. With an incident like a data breach, for example, it may take some time to determine how many customers are affected, and which ones. It may not be possible to quickly obtain the information you'd ideally like to distribute.

Given the speed of the news cycle, consider staffing your media war room with the most senior people available, ones who are empowered to make quick decisions. Have a lean, senior-level approval process in place, and stress test that process in advance.

As you consider the stakeholders you will need to address in your crisis response, don't forget how important your employees are. They can be your best brand ambassadors. They're the ones getting asked the tough questions by friends and family in times of a crisis—and you need them to be empowered to represent your company well. At a tactical level, that flow of communication begins at the top. Give senior leaders information to share with employees in group settings and encourage them to open up a dialogue. Give as much information as possible, and repeat it often.

Outside of your organization, neutral third-parties, like key opinion leaders and influencers, can also play an important role in communicating on your behalf, but these relationships are ones you need to develop and nurture in advance—it can't be done during the height of the crisis.

Finally, consider the global market. The last thing you want is for your teams in another time zone to wake up and find out about the crisis through the media or calls from customers. Consider translation time and distribution networks in your preparations for crisis communications, and be cognizant of the fact that key messages may need to differ by market.

Prepare as Though a Crisis is Imminent

Inevitably in business, there are things you can't plan for, no matter how hard you try. And in a digital world, news of a crisis can spread with dizzying speed.

The time to act is now. We've given you a lot of information and examples of actions you can take related to crisis management, external support and communications, but in the end, the responsibility for crisis preparedness isn't limited to the C suite. News moves fast, and the first and last line of defense is prepared leaders and employees—people who are ready and able to act quickly and agilely when the unexpected inevitably happens.

[1] ICM, ICM Annual Crisis Report, 2017.

[2] Peter Dent, Rhoda Woo, Rick Cudworth, Deloitte Insights, Stronger, Fitter, Better Crisis Management for the Resilient Enterprise, June 18, 2018.

[3] Gallup. The End of the Traditional Manager, May 31, 2018.

Copyright © 2018, Equifax Inc., Atlanta, Georgia. All rights reserved.
Equifax and EFX are registered trademarks of Equifax Inc. 17-7116. This material
is provided for convenience and should not be considered legal advice.