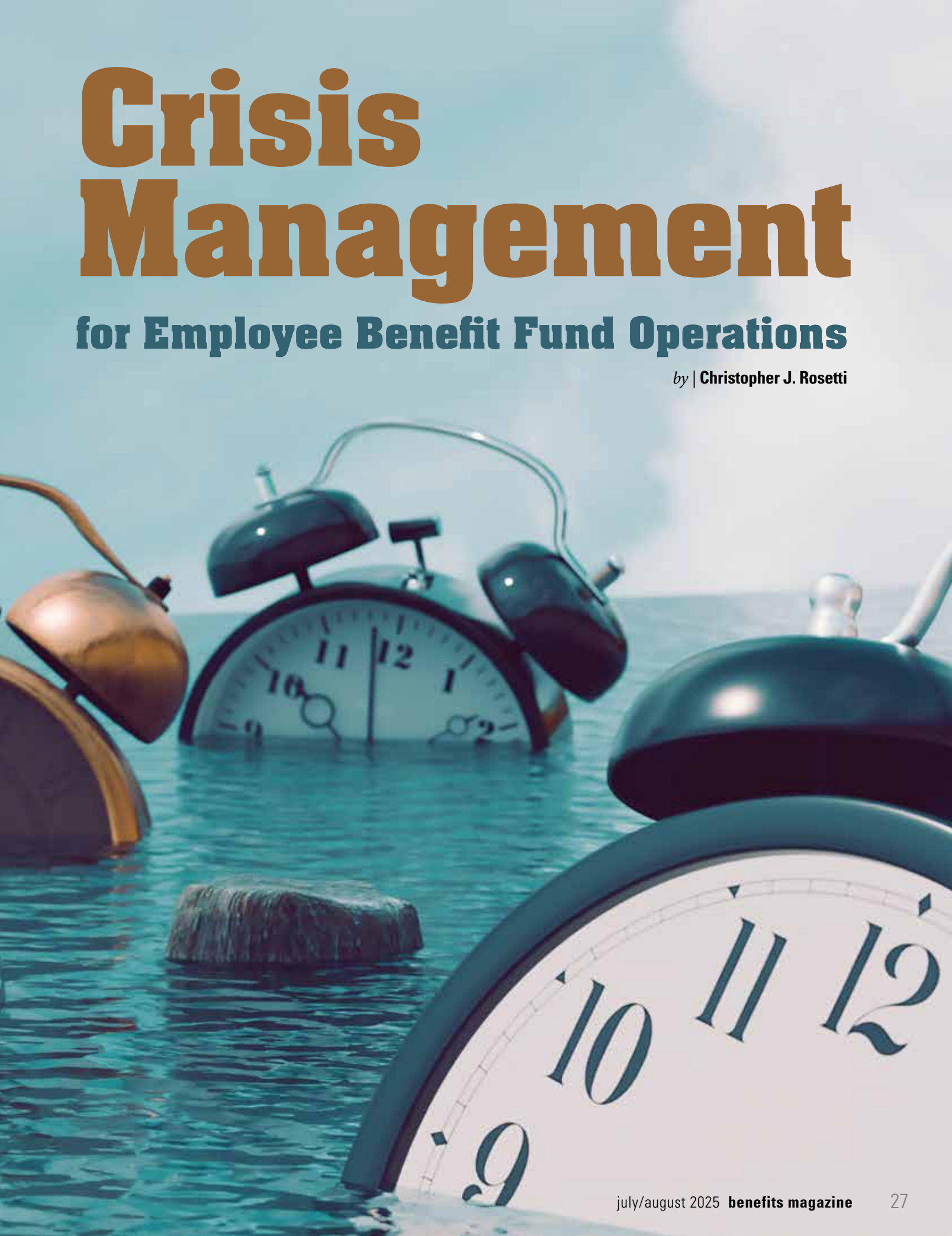
benefits
MAGAZINE

A crisis can occur at any time, without warning and with potentially serious consequences, especially if you are unprepared. Fortunately, proper planning can help your employee benefit plan ameliorate the impacts of these events.

Crisis Management

for Employee Benefit Fund Operations

by | **Christopher J. Rosetti**



During my formative years, my parents frequently told me that sometimes it is best to make a mistake when you are young because you're more inclined to learn from it and, therefore, you tend not to repeat your mistakes.

Well, I made many mistakes and took that wisdom to heart in both my personal and professional endeavors. I shared this lesson recently during presentations I made with a colleague on crisis management for the International Foundation of Employee Benefit Plans.

The crux of the presentation was that it's hard to mitigate a crisis if you don't consider the likelihood of its occurrence—and plan for its possibility. While I don't know this for certain, it's my guess that several organizations didn't have a plan or expect the wide-ranging impact of the fires that ravaged the southern California coastline earlier this year. Furthermore, and based on what I've read, I'm sure many organizations were affected by the epic devastation caused by Hurricane Helene in 2024 as it ransacked communities across the Southeast after its sojourn from the Gulf Coast.

My parents' advice can serve as a lesson in this instance: My hope is that those disaster-affected organizations that didn't have crisis management plans have learned from their experiences and will make sure that they are ready to respond to future disasters.

Costly Disasters

The number of weather and climate disasters causing at least $1 billion in damages climbed to a record level of 28 in 2023.[1] In addition, over the past five years, the number of billion-dollar disasters has averaged 18 annually.[2]

takeaways

- It's difficult to plan for a crisis if you don't know your plan's vulnerabilities.
- Don't reinvent the wheel—Interact with other plan sponsors and learn from their experiences when planning for a crisis.
- Review your insurance policies and evaluate your coverage relating to cybersecurity issues and natural disasters.
- Consider the likelihood of climate-related issues specific to your area and develop a remediation plan in the event of its occurrence.

The dollar amounts notwithstanding, some of the organizations impacted by these disasters suffered significant loss of electronic and other data, which oftentimes paralyzed their operations. Some of these companies never reopened.

Considering this, it likely isn't a question of whether your organization will be impacted by a crisis—but when it will happen.

The reality is that natural disasters (hurricanes, tornados, earthquakes, floods, landslides, etc.) increased by a factor of five between 1970 and 2019.[3] It may be hard to pick a state that is not affected by natural disasters. Texas and California had more than 20,000 wildfires during 2022; Mississippi had approximately 184 tornadoes that year, and the state of Washington had approximately 500 floods in the same year. Florida also led with the most hurricanes, and Illinois was second most at risk for billion-dollar climate disasters.[4, 5]

Given the above, it's incumbent for any pension/welfare benefit fund office to plan for the possibility of these events, not only because they happen, but also because it is your responsibility, and your members are depending on their pensions and health and welfare benefits.[6]

Natural disasters and weather events are not the only risk to benefit plans. Hacking or other cybersecurity events can also be disastrous. For example, 63% of all respondents replying to a survey question during our presentation acknowledged that a cyberattack/hack was the most likely crisis that would impact their pension/welfare fund in the next two years.

Plan sponsors also may be challenged by economic uncertainty, workforce shortages, energy consumption changes, and updates in legislation and regulations.

Fiduciary Duties

It's imperative to remember that all plan sponsors are subject to fiduciary responsibilities under the Employee Retirement Income Security Act (ERISA), including but not limited to the following.

- **Duty of care:** Acting in a prudent manner
- **Duty of loyalty:** Acting in the best interest of the beneficiaries
- **Duty of prudence:** Making decisions concerning the interests of the beneficiaries

Accordingly, your plan should periodically consider the possibility and probability of natural (geologic, clima-

Frequency of Disasters

During our presentation at the Advanced Trustees and Administrators Institute conference in 2024, my colleague and I polled the audience and asked whether their pension/welfare plan had endured a disaster within the past five years. Many audience participants responded yes, and that's not surprising when you consider the number of business continuity issues and disasters that have occurred within the past five years, including but not limited to the following.

The COVID-19 pandemic

The 2021 winter storm in Texas, during which millions of people lost power

Hurricane Ian, which caused $112.9 billion in damages

2023 wildfires in Hawai'i

2024 flooding in Alaska

2024 storms in Illinois

tological, biological) and man-made disasters (terrorism, pollution, nuclear accidents, civil unrest, ransomware, power outages) since any one of these could result in challenges for your organization or business partners. For example, if a crisis affects a vendor that supplies your fund office with items such as paper, toner, etc., you may need an alternate source of these materials to continue sending pension checks, statutory notices and other required documents.

Regardless of the type of disaster, almost every entity faces the same immediate issues when it has experienced one. For example, organizations may need to:

- Restore computer operations
- Find temporary work locations
- Have a method for communicating with staff, participants and business partners
- Retain staff.

Putting Together a Plan

Transitions can not be effectuated without proper planning—Preparation is key.

Risk Assessment

The first step should be conducting a formal risk assessment that considers unexpected occurrences. The risk assessment should evaluate the probability of an event occurring, your vulnerabilities and the potential cost associated with an event. Focus on the areas that result in the greatest costs, such as cyber intrusions, data breaches and theft of organizational assets.

Steps in this process include the following.

- **Set clear objectives.** Establish a deadline and to whom the assessment should be presented.
- **Review insurance policies.** Review your cyber, business owners' and umbrella policies to see what risk, if any, can be potentially assumed by others.
- **Seek assistance from experts.** These might include the plan attorney, insurance broker, mitigation specialists and IT consultants.
- **Gather feedback from staff.** This would include IT, accounting and human resources staff who may have solutions or may be aware of other matters that management hasn't considered.
- **Identify available resources.** It also doesn't hurt to reach out to others and learn what they experienced during a crisis, since these organizations are likely to have some practical advice.

Crisis Management

After assessing the risks, the plan should cover how a crisis will be managed. Essential elements of crisis management include the following steps.

- **Identify internal hazards and risks.** It is often helpful to consult with other plans to see what they have experienced and how they resolved the issues.
- **Communicate risks.** Periodically remind staff of the risks, specifically cyber-risks and the red flags of fraud, and how they can be avoided. Prudent practices dictate sharing knowledge and information with your staff so that they are aware of current trends and schemes.

- **Mitigate consequences.** Assume, transfer or mitigate the risks once they have been identified. Most organizations transfer the risk by obtaining the required insurance, and others also mitigate these risks by implementing rigorous internal controls. Still, others assume these risks by self-insuring or taking the gamble that certain occurrences will never happen.
- **Restore trust.** Working with staff to reach a common goal instills a sense of pride between the team members and is instrumental during times of crisis as the plan members realize their benefits have been unaffected or timely restored.

Focus on Business Continuity and Recovery

Finally, your plan should address ensuring that the organization's operations can continue and recover after a crisis has occurred. Some of the key areas to address in business continuity include the following.

- **Communication:** Your plan needs to ensure that communications won't be interrupted. Using phone applications that can be downloaded on personal cell phones is one option since they generally aren't impacted by power outages (i.e., your cell phone can receive calls originally directed to your plan office phone system and your desk phone).[7] Make sure that the fund has current telephone numbers and email addresses in order to send emails or phone blasts. Consider providing an online Q&A if phone lines are down. Lastly, having a social media site can be instrumental in communicating messages to the masses in the event email capabilities have been compromised.
- **Continuity of power and access to information:** Many institutions that have been through these situations have lessened their risk of power interruption by leasing a generator as part of their facility rental agreement, and/or they utilize off-site premises or a colocation for data storage. As such, they are almost always immune to some of the issues associated with disasters. During one recent International Foundation presentation, 100% of the attending participants who responded anonymously reported that their organization utilized a colocation for their electronic systems or had off-site storage of electronic information.
- **Access to equipment:** Another common recipe for survival is to have spare computer/phone equipment that can be used remotely if staff are unable to access the office or if the office is irreparably damaged.
- **Maintaining confidentiality:** If staff are temporarily working off site, plans should work to ensure that the confidentiality of health information required by the Health Insurance Portability and Accountability Act (HIPAA) is maintained. This can include reminding employees to work from a secure, private location and not their kitchens or directing the IT department to program laptop and PC screens to lock after five minutes of inactivity. More importantly, directives should also include prohibitions against printing work material at home. Simply put, your IT department should disable any printing capabilities of the PCs and laptops provided to your staff if they are going to work remotely. The latter issues are important at all times, since many people continue to work remotely either full-time or on a hybrid schedule following the COVID-19 pandemic.
- **Information security:** The security of physical documents when the office space has sustained physical damage is of equal importance. On-site confidential information needs to be safeguarded against unsavory individuals who prey on organizations exposed to disasters. Plans should consider eliminating paper documents to the extent possible and scan documents instead to ensure access to data. You need to ask yourself what type of security can be retained on short-term notice in the event of an unexpected crisis.

Conclusion

Most plan sponsors generally have an acute awareness of their current exposure, reinforced by historical events and their geographic locations. Further, it's hard to imagine that the plan sponsors don't have insurance policies in place to mitigate their risk. However, taking the steps suggested in this article is an additional and likely necessary strategy to

help your plan assess what is needed to sustain operations and minimize damage in times of crisis.

Endnotes

1. "2023: A historic year of U.S. billion-dollar weather and climate disasters." NOAA Beyond the Data blog.
2. Penny Gusner, "Natural Disaster Facts and Statistics 2025," Forbes Advisor.
3. Joelle Goldstein, "Deadly Natural Disasters Have Increased Five-Fold Over 50 Years Due to Climate Change," *People Magazine*. September 1, 2021.
4. Penny Gusner, "Natural Disaster Facts and Statistics 2025," Forbes Advisor.
5. Twenty percent of the audience surveyed noted that they live and work in California or Florida.
6. Twenty percent of the respondents during our crisis management session said that their pension/welfare plan endured a disaster/business continuity issue within the past five years.
7. These applications are available through voice over internet protocol (VOIP) options such as Ring Central.

pdf/725

bio

Christopher J. Rosetti, CFE, CFF, CPA, is the chief operating officer of the New York State Nurses Association Pension Plan and Benefits Fund in Albany, New York. He was previously a partner with BST Valuation and Litigation Advisors, LLC, and has more than 40 years of diversified accounting and governance responsibilities. He is a certified public accountant, a certified fraud examiner and certified in financial forensics. He holds a bachelor's degree in business administration from Siena College and a master's degree in public administration from Rockefeller College of Public Affairs and Policy at the University at Albany. Rosetti can be reached at CRosetti@rnbenefits.org.