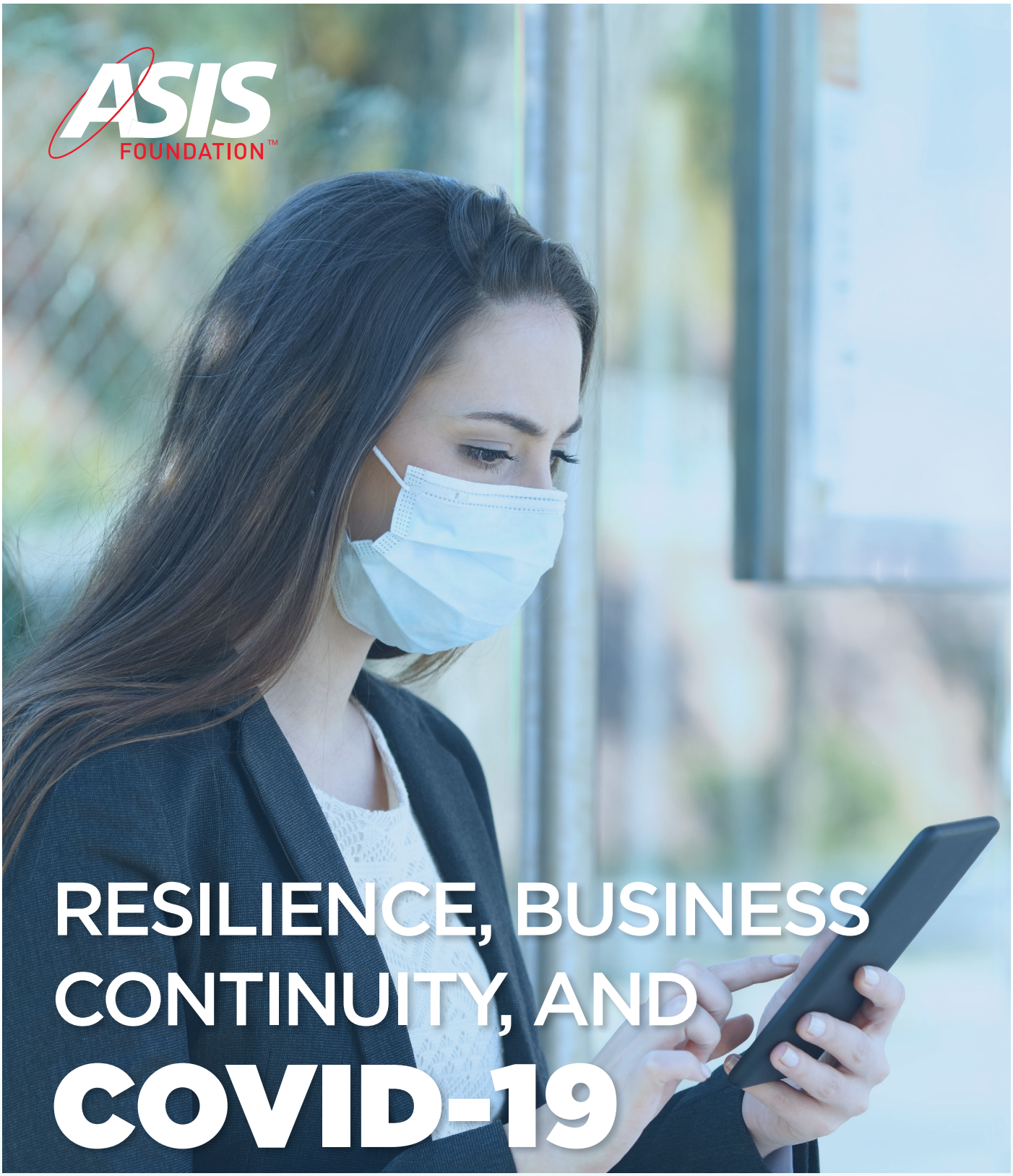

ASIS
FOUNDATION™
RESILIENCE, BUSINESS CONTINUITY, AND
COVID-19

Table of Contents

Executive Summary and Key Takeaways 3

Implementing a Plan for COVID-19 5

Crisis Management, Resilience, Business Continuity: What Lives Where? 6

Structural Changes to Resilience and Business Continuity 7

Changes of Duties Due to COVID-19. 7

Successes 8

Case Studies of Two Financial Institutions 11

Opportunities for Improvement. 13

Lessons Learned 14

Appendix I: Summary of Nonnarrative Survey Responses. 15

Appendix II: Glossary of Key Terms. 17

About the Author

Michael Gips, JD, CPP, CSyP, is the principal of Global Insights in Professional Security, a firm that specializes in knowledge management, content creation, research, business development, and thought leadership for security departments, service providers, manufacturers, and other organizations. He was previously Chief Global Knowledge & Learning Officer at ASIS International. Prior to that role, he served as Vice President of Publishing, Vice President of Strategic Operations, and an editor at Security Management magazine. Gips's previous work for the ASIS Foundation includes reports on convergence, blockchain, and COVID. He also publishes security research with other organizations, frequently presents at conferences and webinars, and hosts a security podcast.

ASIS International | 1625 Prince Street | Alexandria, Virginia, USA 22314

EXECUTIVE SUMMARY AND KEY TAKEAWAYS

The COVID-19 pandemic tested businesses and security teams in new ways. It highlighted the importance of having a solid business continuity plan supported by senior management that is updated and exercised regularly. Companies with good communications, strong leadership, and a resilient staff fared the best.

This report is the culmination of COVID-19 research that the ASIS Foundation initiated in March 2020. The original research studied nine companies in detail, tracking their pandemic response and recovery efforts from March through December 2020. Participants included: a U.S.-based NGO working primarily in Africa; a global bank based in Canada; a polymer-manufacturing company headquartered in Europe; a U.S. food and agriculture company; the Asia-Pacific region of a global furniture retailer; a global chemicals conglomerate based in Europe; a microfinancing institution serving Mexico and other Latin American companies; a polytechnic institute in southeast Asia; and a clothing retailer based in the United States.

A series of articles updated the efforts of each organization to adapt to the massive disruption wrought by COVID-19. The pandemic precipitated an unprecedented shift from office work to remote work, raising new cybersecurity and duty-of-care issues. It also shut down travel, required vigorous new sanitization protocols, introduced the concept of social distancing, imposed occupancy limits, and brought health screening and face masks to the workplace. Of course, different industries were affected in different ways. For example, retailers pivoted to online sales, while factories were forced to continually deep clean, rotate shifts, conduct contact tracing, and take other measures to make sure the world had sufficient food, toilet paper, and cleaning products. Key learnings from the various industry sectors can be found **here**.

This report concludes that research by exploring the following questions:

- When COVID-19 hit, did the organization implement a crisis management or business continuity plan? How did it fare
- How has resilience and business continuity planning changed structurally as a result of COVID-19?
- How have the resilience and business continuity duties shifted during COVID-19?
- What have organizations done well in this crisis?
- Where do organizations have room to improve
- What other lessons have been learned or insights gained to help organizations better prepare?

To address these issues, the researcher followed up with the nine original companies, conducted a literature review, fielded a survey of senior security executives, and interviewed several of the survey respondents. One hundred and nineteen people completed the survey. Results and conclusions follow. A summary of the survey results appears in Appendix 1.

Many of the terms used in this report have similar meanings or meanings that vary by organization. For clarity, Appendix 2 provides definitions of these terms from ASIS International standards.

KEY TAKEAWAYS

Terminology

- Organizations often have specific meanings for terms such as resilience, business continuity, crisis management, disaster recovery, and so on. And those meanings are not necessary consistent from organization to the next.
- Other organizations, however, use these same terms loosely and interchangeably.

Business Continuity and Crisis Plans

- When COVID-19 arrived, most companies implemented a plan they had in place. However, 43 percent of companies either had no plan, ignored the plan, or made limited use of it.
- Even most companies that used a plan and hewed to it found that it did not adequately contemplate the effects, magnitude, and length of the COVID-19 pandemic.
- Plans that are not regularly reviewed, contemplated, updated, and exercised diminish in value.
- Effective business continuity and resilience rely on support—and even robust advocacy—from the top. Absence of executive support cripples resilience, business continuity, and crisis management efforts.

Structural Changes to Business Continuity and Resilience

- Forty-one percent of the survey respondents said that COVID-19 had triggered structural changes to the resilience or business continuity functions. Fifty percent said they had not, and nine percent said that those functions reside in individual business units.
- The structural changes that have occurred are sui generis and cannot be easily categorized.
- Many companies are still examining and processing their resilience programs and will make changes consistent with recommendations that emerge.
- Various respondents say that their organizations are considering shifting business continuity to corporate security.

Change of Duties Due to COVID-19

- Nearly 40 percent of survey respondents said duties or responsibilities of the resilience or business continuity team have changed because of the COVID-19 pandemic.
- The most common change is that their resilience or business continuity team added health and safety duties where none existed before.
- The next most cited change is that senior executives better understood the importance of business continuity planning, crisis management planning, and conducting exercises, and now better support those activities.
- In some cases, the pandemic has vested additional aspects of crisis and continuity planning in the security department.
- Some resilience teams broadened their scope of duties; others had it narrowed.

Pandemic Planning and Response Successes

- Respondents cited 35 discrete successes in dealing with COVID-19.
- The most cited success was communicating effectively and frequently throughout the organization and beyond, followed closely by transitioning to remote work.
- The next two frequently mentioned successes included:
  - Ensuring staff safety/upholding duty of care
  - Implementing building safety protocols including occupancy limits, social distancing, cleaning and disinfecting regularly, and providing personal protective equipment
- Other successes that registered included:
  - Keeping the business running/finding new markets
  - Responding quickly to the crisis
  - Collaborating with internal and external stakeholders
  - Pushing response to the local level
  - Adapting/protecting the supply chain
  - Providing financial assistance for staff or furloughed workers

Opportunities for Improvement in Pandemic Planning and Response

- Respondents cited as many distinct areas for improvement—35—as they did successes.
- Most common areas for improvement included the need for better or more frequent communications.
- Four other challenges frequently cited were:
  - Lack of a more useful, more specific, or more updated business continuity plan—or even a plan at all.
  - Difficulty in shifting to remote work
  - Slow response
  - Lack of devoted resources

Lessons Learned

- Almost 50 different lessons learned were identified.
- The most frequently mentioned were:
  - The importance of communication, flexibility, teamwork, and leadership
  - The ease or difficulty of shifting to telework (about as many security executives were surprised by how well they fared as found the process difficult)
  - The importance of preparation and having a plan
  - The importance of resilient staff
  - The value of consulting with, retaining, or hiring medical experts such as virologists, epidemiologists, nurses, and qualified health-check screeners
  - The need to take care of isolated staff who might be lonely or struggling with mental health issues

Implementing a Plan for COVID-19

Typically, the first step in addressing a crisis is implementing a preexisting plan that has been updated and periodically exercised, and in which tasks or responsibilities have been assigned to specific roles or individuals. Fifty-seven percent of survey respondents said that they implemented some sort of preexisting business continuity, resilience, or crisis management plan when the pandemic. Another quarter put at least part of their plan into action. Four percent didn't take their plan off the shelf, and 12 percent lacked a plan altogether.

That means a total of 43 percent of respondents either had no plan, inadequate plans, or plans that were not even worth consulting. Many organizations put little thought into pandemic planning.

Of the organizations that executed a plan, some had generic plans while others had plans, or significant sections of plans, devoted to pandemics. But even in the latter cases, almost no one's plan contemplated the scope and duration of the disruption wrought by COVID. "We used the pandemic section of our overall plan," says the CSO of a $1 billion financial institution. "However, additional measures were added due to the magnitude of the event." Another financial institution was in the midst of updating its plan for infectious diseases when COVID arrived. It resulted in a situation akin to putting the finishing touches on an airplane while it is in flight.

A power company based in Europe had developed a comprehensive set of policies, procedures, and protocols based on earlier pandemics such as H1N1, SARS, and MERS. But "the scope of COVID-19 forced a lot of changes, monitoring and collating of information and impacted business on a global level," according to the head of security.

The head of security for a manufacturer notes that his company used a plan that was developed in 2009 in response to H1N1. "It generally serves us well, but it did not address things like maintaining PPE inventory or temperature screening, and did not embrace our current concept of operations," he explains.

The common theme is that plans that are not regularly reviewed, contemplated, updated, and exercised diminish in value.

Those without pandemic-specific plans appear to have lagged behind their better-prepared counterparts, but not by much. Security executives reported quickly getting their response into gear. "For us, things happened incrementally," says the CEO of an Australian security services firm. "So we put parts of our normal business continuity plans in action, and then we developed COVID-specific plans. Some of our personnel are embedded

within client projects, so they had to have a mix of client and company plans."

The response of the CSO of a U.S.-based manufacturer is illustrative. "We had a robust and exercised BC plan, but it didn't specifically address a COVID-19-like situation. However, all stakeholders were able to readjust quickly to address concerns presented."

And, according to the collective survey responses, those main concerns included shifting to work at home and adjusting to changes in logistics and the supply chain. But many plans, including pandemic-specific ones, failed to contemplate the duration of the crisis, forcing companies to adapt on the fly.

Another significant finding is that effective business continuity and resilience rely on support—and even robust advocacy—from the top. Leadership at one U.S. food manufacturer stymied crisis management and continuity efforts, according to the CSO. "We failed to engage in crisis planning and reenergize the corporate crisis plan," the CSO laments. "The plan is a top-secret document that isn't well known and wasn't activated during COVID. It still sits on a shelf. Few people have even looked at it, and it hasn't been exercised since 2017." In that company, the CEO created a crisis team independent of the plan. While the team performed admirably, it ignored the existing plan. "I called it out to the executive team that we should have used the plan to go forward," he recalls. "But no one wanted to bring it up to the CEO. I can't drive something in the absence of an executive sponsor."

CRISIS MANAGEMENT, RESILIENCE, BUSINESS CONTINUITY: WHAT LIVES WHERE?

Organizations sometimes use terms such as crisis management and business continuity interchangeably, while others have specific definitions. But those definitions do not necessarily match from company to company. In addition, these functions are often fragmented across various departments.

Consider for example the security and resilience department of a technology company. It owns emergency response preparedness and business continuity planning. While security drives business continuity, the individual business units that own critical functions are responsible for the development and implementation of business continuity. Security provides subject matter experts and helps with the business impact analysis. The company has three types of plans. Emergency response plans cover fires, evacuations, and the like. Crisis management plans deal with longer disruptions, such as power outages and weather emergencies. The business continuity plan kicks in for prolonged crises.

Contrast this approach with that of a global retailer. It has 140 separate business continuity plans based on critical processes and issues such as payroll, single-point-of-failure vendors, and key facilities. The crisis management process, which is separate from business continuity, involves 60 people representing safety, HR, facilities, and various other departments. The company plans to place preparedness, continuity, and resilience in a single department.

Meanwhile, one financial institution has a business resilience unit that oversees crisis management, data governance, operational risk management, and disaster recovery. These functions sit separate from security.

At another financial institution, an enterprise risk management department contains crisis management and business continuity. It reports to finance, not to security. Finally, another organization embeds separate continuity teams in each business unit.

Structural Changes to Resilience and Business Continuity

When asked whether the pandemic has occasioned structural changes to the resilience or business continuity functions, the respondents split down the middle: 50 percent said no, 41 percent said yes, and nine percent said that the functions reside in individual business units.

One large European pharmaceutical company used the crisis to make significant changes. "We have revised planning to focus on the value chain and make BC requirements optional for commercial divisions based on assessment of risk," says the head of security. Business continuity and crisis management moved from health and safety to risk and compliance in early 2020, he adds.

In some cases, security got invited into the business continuity tent after having been historically excluded. That was the case at a North American chemical manufacturer, which previously had minimal involvement in continuity issues. Not only is security in the tent, it now owns the tent. "Corporate security has been given responsibility for business continuity" for everything except IT, reports the CSO.

Other organizations have held back but are poised to make changes. "Our business continuity team is leading an effort to formalize an operational resilience function that will lead to a broader mandate for that team," notes the head of continuity for a North American financial institution. "The business continuity team has been driving operational resilience for several years, and we are taking this opportunity to formally broaden their responsibilities," he adds.

Various respondents say that their organizations are considering shifting business continuity to corporate security. In those companies, business continuity resides in such departments as safety, IT, operations, or risk management.

Another group of respondents did not make structural changes, but because the COVID-19 pandemic has been all-consuming, they assigned business continuity to individual business units. Such was the case at a public university in the northeastern United States. According to the head of emergency management, "departments had to take on their own implementations and strategies. They had to do whatever was necessary for remote work and so forth. They did this organically" without it being part of any plan.

Changes of Duties Due to COVID-19

Slightly more than 38 percent of survey respondents said that the duties or responsibilities of the resilience or business continuity team changed because of the COVID-19 pandemic. Most of the rest of the respondents said they had not changed. (The remainder said that they did not have a distinct resilience or business continuity department.)

of resilience and business continuity teams say their duties changed due to COVID-19

Without being offered options or prompts, respondents were asked to narratively describe those changes. About one-third of those responding indicated that their resilience or business continuity team added health and safety duties where none had existed before. A very large financial institution, for example, "expanded

well beyond traditional BCP work—managing health monitoring globally, driving all aspects of work from home, return-to-office process, building process around testing employees, field protocols for contact with clients, and PPE [personal protective equipment] protocols."

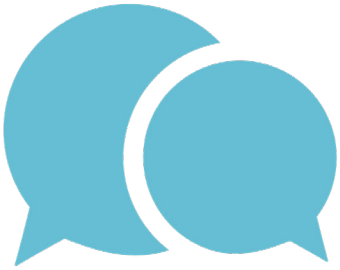
An energy company added a COVID-19 medical advisor to the business continuity team, while a security service provider has added health and safety monitoring, which has required more staff training. And the CSO for a financial services firm says that the business continuity team "has expanded well beyond BC and security work, from health and safety work to establishing policy and process for COVID testing across the organization."

The move to more health and safety roles was not uniformly applauded. One security executive notes that business continuity focuses exclusively on the COVID-19, suggesting that the company lacks the resources to effectively deal with other types of crises, such as wildfires, floods, or long-term Internet outages.

Respondents also reported more general changes to their resilience or business continuity groups. Senior leaders better understand the importance of business continuity planning, crisis management planning, and conducting exercises. "I foresee less pushback on tabletops and annual reviews of our plans," says the senior security executive at a chemical manufacturer. "It also has the attention of the board, which doesn't hurt."

In a few cases, the pandemic has vested additional aspects of crisis and continuity planning in the security department. "We became the drivers of the business continuity management program, with more authority," says the head of security for a technology company.

In some instances, the resilience team broadened its scope; others saw their focus narrowed. For example, the security head at a manufacturer observes that the team initially dealt with processes and tools for the business units, "but during COVID the team responsibilities evolved to lead the response in coordinating action items across all key functions." By contrast, at a pharmaceuticals company, business continuity is now optional for all business units except those for which business continuity is deemed essential: supply chain, manufacturing, clinical trials, and backbone services.



Effective communication is both the most cited success and the most cited failure of pandemic planning and response.

Respondents identified several other ways duties shifted. Because of the duration of the pandemic, at least one company offloaded responsibilities from the business continuity management team to other departments. Others identified increased collaboration between teams. Still another added a business resumption committee and a COVID-19 enforcement committee to its business continuity plan.

Many companies are sifting through lessons learned before altering functions or shifting responsibilities. At one large retailer, the preparedness, continuity, and resilience teams have different reporting lines. They likely will be merged into a single department going forward.

Successes

Where did crisis and resilience planning, testing, and execution pay dividends? And what do companies think they did well in dealing with the COVID-19 pandemic? Security executives were invited to supply their own narrative replies, and they offered a wide array

of responses, ranging from doing nothing right to doing everything well.

Respondents identified at least different 35 actions that they performed well. Cited most frequently were communicating effectively and frequently throughout the organization and beyond (20.6 percent), transitioning to remote work (18.7 percent), ensuring staff safety/upholding duty of care (15.9 percent), and implementing building safety protocols, including occupancy limits, social distancing, cleaning and disinfecting regularly, and providing personal protective equipment (14 percent).

Other items registered in significant numbers as well. They included keeping the business running/finding new markets (6.5 percent), responding quickly to the crisis (6.5 percent), collaborating with internal and external stakeholders (5.6 percent), pushing response to the local level (5 percent), adapting/protecting the supply chain (4 percent), and providing financial assistance for staff or furloughed workers (4 percent).

The following are examples of some of the most frequently mentioned successes.

Communication

No crisis response can succeed without timely, trustworthy communications to staff and outside stakeholders, such as partners, contractors, and shareholders. So it is no surprise that communication tops the list of things done right.

Communication is critical because it establishes credibility and transparency, according to the CSO of a U.S.-based defense contractor. "We kept the staff informed of what was going on, even though we weren't even sure ourselves," the CSO says. "We at least told them what we knew." To that end, the C-suite updated staff with information at least twice weekly, and the company set up an online question/comment box. "People felt like we were doing everything we could," says the CSO, who adds that the company quickly responded to requests for hardware such as monitors or headphones.

The head of security at a Europe-based technology company applauds the firm's streamlined, accessible crisis-communication system. After every weekly leadership meeting on the status of the pandemic and its impact on operations, information is updated on a corporate intranet page. It addresses issues such as the return to office playbook, travel policy, site status, work-at-home guidelines, and site access policy.

The power of effective communication to staff and other stakeholders becomes clear in the results of a survey recently conducted by a financial institution. "Survey results have shown that both employees and customers have appreciated the level of communication provided and clarity on requirements," according to the CSO. "Through feedback, we have heard that other organizations within our line of business have not been as transparent, which caused anxiety."

Remote Work

Many executives commend their organization's speed and effectiveness in deploying a remote workforce. In many cases, companies had to buy new devices or take old ones out of mothballs. They then needed to add or update software, including security tools such as antivirus and anti-malware, and distribute the technology to thousands of workers—many of whom may have already been advised to stay home. IT would also have to ensure that the network infrastructure could support such a heavy remote burden, that enough VPNs were in place and intact, and that staff understood policies and procedures for remote work, such as securing and regularly changing passwords, sharing devices with family members, and accessing corporate data from personal devices. Finally, teleworking staff might have hardware, software, ergonomic, or connectivity issues that needed attention.

"We were quick out of the box," explains a CSO of a financial services company that transitioned quickly to working at home. "I told my team to work remote a week before the company told the rest of the staff to do so. We have a small team and couldn't afford for people to get sick."

Key to that transition was investing in cyber infrastructure, including strengthening the VPN. Equally crucial was that staff use laptops, not PCs. They could easily take their laptops home and already knew how to use them. Further, all software had been updated and staff trained. The only downside was that "there was a mad scramble for monitors, but that's it," per the CSO.

The northeastern U.S. university had a similar experience. "We did a great job of quickly enabling remote work by a workforce of some 10,000 people," recounts the head of continuity. "Part of what made this successful was that the IT department already worked remotely every week for at least one day."

Staff & Facility Safety

Almost 16 percent of respondents praised their organizations' focus on staff safety and attention to duty of care, naming workers as their key asset. The security director of a South American financial institution credits the organization's collection and distribution of reliable information and implementation of safety training and health protocols for its minimal infection rate and absence of mortalities.

Relatedly, almost as many respondents lauded their facility safety efforts. They include health checks, deep cleaning, PPE distribution, staff schedule changes, office reengineering, HVAC adjustments, occupancy limits, directional markings, sanitization stations, and distribution of sanitary keys (devices used to enable contactless door opening or button pushing), among others.

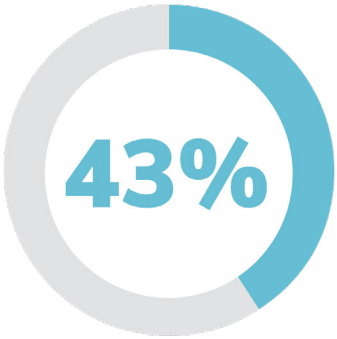
Much of a defense contractor's work must be conducted in a sensitive compartmented information facility (SCIF), a secure space in which to view and discuss sensitive information. That creates a twofold problem: having staff regularly come to the office, and keeping staff safe inside cramped SCIFs. Defense contractors have introduced health screening and temperature checks at the front door, which are usually conducted by security officers. They also enforce social distancing and elevator occupancy limits and rigorously clean the facility. One defense contractor respondent posts occupancy limits on each conference room and SCIF door. It also has adjusted air flow in the SCIFs and other tight areas to reduce the chance of virus transmission.

Data Modeling: A Singular Success with Broad Applications

The CSO of one manufacturing company describes how the data science team built advanced data models of disease transmission and their effect on staff travel, return to and departure from sites, and other outcomes. The company has provided these tools to hundreds of other companies.

It started early in COVID with the confusion around which airlines were operating and which countries had changed border control rules. "Countries were changing on a dime," the CSO says. A regional security director built a tool to track those concerns, which got the attention of the crisis management team.

In March and April, security was warning of rampant disease spread in Europe and the Middle East. "The only way to get [the corporate management team's] attention was to show them hard data, that it was undeniable that the wave was coming," the CSO recalls. The data science team built models that showed disease-spread projections for Asia-Pacific, Italy, Spain, France, Israel, and other countries, The company has continued to rigorously refine the model, fixing any discrepancies. The latest iteration calculates risk scores, with scores triggering such actions as site opening/closure or cessation/resumption of business travel.



of organizations reported either not having a business continuity plan or using it only minimally.

CASE STUDIES OF TWO FINANCIAL INSTITUTIONS

Two North America-based financial institutions reported a wealth of findings related to successes, opportunities, and lessons learned. Below are examples from each.

Successes (Institution 1)

- Corporate incident management response was proactive.
- Tactical and strategic teams were widely accepted as key decision-making bodies for response efforts.
- Trust and credibility were established among the response team prior to COVID; that was critical in the ability to collaborate and drive forward through uncertainty.
- The company quickly pivoted in response to each issuance of new guidance from public health and governmental authorities.
- Incident management roles were well understood due to training and exercises over past years.
- Previous investments in technology to support remote work paid off.
- Investment in multiple operational sites paid off.
- Establishing guiding principles for response efforts led to consistent application of tactical decisions.
- Communication was clear, concise, and frequent.
- Capacity issues were anticipated in advance.
- Staff received an allowance to ensure home offices were adequately outfitted for productivity and comfort.
- Telework exercises in prior years allowed a seamless transition to full telework.
- Response leaders made regular outreach to peers for benchmarking.

Successes (Institution 2)

- Expanded from primarily business/office risks to both office and home and community risks (e.g. social unrest, wildfires, hurricanes, power outages).
- Monitored social unrest country-wide as it pertained to offices and employees' homes.
- Secured potential hot spots and quickly addressed damage done to several properties.
- Accelerated improvements to network infrastructure and purchased additional laptop computers and peripherals.
- Quickly and efficiently set up 98 percent of institution's more than 10,000 employees to work from home.
- Crisis Management Team engaged in late January and ran multiple concurrent workstreams well into June, creating a new, virtual workplace that provided employees with the tools and support they needed to remain almost 100 percent productive.
- Crisis Communication Plan paid great attention to immediate and ongoing communication and transparency.

- Senior leaders, business unit heads, department, and line managers executed on the crisis communication and transparency plans across the company; within departments, business units, and teams; and in one-to-one communications.

Opportunities for improvement (Institution 1)

- Continue to be mindful of employee concerns and balance the need for quick communications versus need-to-know information and privacy.
- Policy on disclosure or what to do when an outbreak occurs is needed early (employee awareness/ what can I expect to know from an employee perspective?).
- Continue to be mindful of incident response team members' time and encourage a regular rotation of primary and alternate participation and to promote the value in utilizing their operational response teams.
- Consider a simple project management approach for response-related initiatives.
- Provide additional clarity to leaders on how to support employees at home who are caring for children or aging parents, or are dealing with other personal challenges.
- Provide specifics to work hour policies for managers and employees to help ensure a more equitable approach to ensure that the support provided to employees is consistent and fair across all departments.

Opportunities for Improvement (Institution 2)

- Some processes had a single point of approval, which in busy times is also a single point of failure.
- We could have delegated some routine actions or decisions better.

Lessons Learned (Institution 1)

- Our response has highlighted the importance of coordinating resilience initiatives across the organization.
- Business continuity should not be seen as a compliance function, but one that ventures into assurance through partnerships with business units and a shared understanding that business continuity planning and resilience initiatives need to be an organizational priority.
- Avoid placing undue emphasis on hot topics (e.g. ransomware) at the expense of broader or lower likelihood scenarios such as infectious diseases

Lessons Learned (Institution 2)

- While some crises are not completely predictable, regular, or transparent, communication from leadership was key.

Opportunities for Improvement

Security executives were asked to describe, through narrative responses without prompts, what they could have done better in their COVID preparation and response. They identified about as many of these opportunities—35 or so—as they did successes.

Six items appeared most frequently. Better or more frequent communications garnered the most mentions (16 percent). Another 14 percent of respondents lamented not having a better, more specific or more updated business continuity plan—or even a plan at all. About 12 percent said there was nothing they could have done better. Shifting to remote work frustrated nine percent of respondents, an equal amount despaired that their organization didn't act quickly enough, and six percent said that more resources could have been devoted to the effort.

Below are details on a few of the most frequently mentioned items.

Communication

Communication concerns were far from uniform. A university executive says that the lack of a mature business continuity program impeded centralized communications to staff. A utilities CSO notes that effective communications to outside stakeholders at the onset broke down as the pandemic dragged on: "We couldn't sustain partner and client engagement," the CSO laments. "We started off really well, but as the pandemic transitioned from novelty to standard practice, engagement and communication waned a bit." Others saw opportunities to make staff communications more user friendly early on, to better explain the business continuity process, and to issue more frequent communications.

Plans and Planning

Respondents described various concerns about their continuity plans, ranging from not having one to not including a pandemic section or annex. "The corporate plan was more focused on things other than a pandemic, which can last a long time and affect all offices worldwide," says the CSO of a U.S. defense contractor. "Planning for a pandemic would have helped."

The head of security for a European technology company describes having an excellent crisis management plan in hard copy. "We tested it, put it through the wringer, and everything worked well," he says. "But when we got to the actual crisis, no one looked at the paper plan. They wanted it digitally." And many assumptions in the plan turned out to be wrong, such as certain personnel needing access to a facility—they did fine remotely.

One property management firm not only lacked a business continuity plan, it could have benefited from investing in a crisis management team and a risk register. The CSO of an engineering firm observes that the company lacked a playbook for the pandemic and could have used "more proactive planning and crisis level training." And the head of security for a food/agriculture company, in retrospect, would have insisted on having a pandemic annex in the business continuity plan.

And what happens if you have a plan but no one knows what their responsibilities are? The CSO of the same food/agriculture company adds that during the pandemic many members of the original crisis management team had retired or moved on from the company. "We lost knowledge, continuity, experience, and information," he says. "The replacements were left with only the documents. They're starting from scratch. And in some cases, replacements haven't been hired."

Other Opportunities

Besides improving the shift to telework, acting faster, and devoting additional resources, respondents noted a long slate of misses and opportunities. Among the dozens mentioned, in roughly descending order, taking the crisis more seriously at the outset, providing better leadership, giving security a seat at the table, accessing sufficient PPE, and adapting to a changing market. Other security executives called out the need for keeping up with health guidance, distributing crisis management templates to individual sites, better managing incoming intelligence, and avoiding the temptation to return to normal too soon.

Lessons Learned

Not surprisingly, many of the lessons learned by respondents echoed their comments about successes and failures. But the lessons identified were much more disparate than the achievements and the areas for improvement. In fact, although far fewer respondents included lessons learned, they identified almost 50 of them—more than either successes or failures.

Most commonly cited were the importance of communication, flexibility, teamwork, and leadership; the ease or difficulty of shifting to telework (about as many security executives were surprised by how well they fared as found the process difficult); the importance of preparation or having a plan; and the importance of resilient staff.

Several members emphasized the value of consulting with, retaining, or hiring medical experts such as virologists, epidemiologists, nurses, and qualified health-check screeners. An equal number stressed taking care of isolated staff who might be lonely or struggling with mental health issues. Other notable lessons included:

- *"We just weren't ready."*
- Intelligence/information, correctly distributed, is indispensable.
- COVID dwarfs other pandemics that triggered previous crisis plans.
- Difficult to distribute PPE globally.
- Balance safety protocols with business objectives.
- *"We were more resilient than we thought."*
- Exercise your plan.
- *"Tabletop, tabletop, tabletop."*
- Culture is key in a crisis.
- Focus on impacts on manufacturing, supply chain.
- Implement business continuity governance across all regions and facilities.
- Less business continuity, more crisis management.
- Security was under-resourced for this pandemic.
- Finance should be represented in the incident command.
- Network with security and continuity professionals from other organizations, but don't wait for other organizations to act first.

This report cannot possibly address every aspect of COVID resilience efforts and programs, but it offers a glimpse of some of the most significant strengths, weaknesses, opportunities, and threats. The pandemic and the prolonged disruption it caused offer security, crisis, and continuity professionals a rare chance to be front and center with leadership and effect change. "This is the best risk management experience that any of us will go through in our lives," predicts a retail CSO.

"The best thing you can do know, if you own resilience, is to not waste the crisis that's in front of you," counsels a manufacturing CSO. Just as attention to terrorism soon waned after 9-11, the pandemic will eventually become a memory. "While there's still enthusiasm around this, get the issue in front of executives to build what you need to be prepared for the next crisis," the CSO continues. "Use your time and energy right now to articulate an argument in terms of organization, reporting, resources, and how to do better next time." ■

Appendix I: Summary of Nonnarrative Survey Responses

1. WHICH OF THE FOLLOWING BEST DESCRIBES THE PRINCIPAL INDUSTRY OF YOUR ORGANIZATION?

a. Conglomerate of Diversified Services 0%
b. Cultural Institutions 0%
c. Defense Contracting 3.51%
d. Education 4.39%
e. Engineering/Construction 1.75%
f. Entertainment & Leisure 2.63%
g. Finance & Financial Services/Insurance 20.18%
h. Government 3.51%
i. Healthcare & Pharmaceuticals 7.89%
j. Law enforcement 1.75%
k. Manufacturing 14.04%
l. Nonprofit 1.75%
m. Retail 4.39%
n. Real Estate/Property Management 0.88%
o. Security Services 9.65%
p. Telecommunications, Technology, Internet & Electronics 7.89%
q. Security Services 9.65%
r. Telecommunications, Technology, Internet & Electronics 7.89%
s. Transportation & Delivery/Logistics 4.39%
t. Utilities, Energy & Extraction 6.4%

2. WHAT IS YOUR ORGANIZATION'S ANNUAL REVENUE

a. Under $100M 11.21%
b. $100M - $500M 12.93%
c. $500M - $1B 15.52%
d. $1B - $5B 21.55%
e. $5B - $10B 6.90%
f. $10B - $20B 6.90%
g. $20B - $50B 10.34%
h. >$50B 14.66%

3. WHEN COVID ARRIVED, DID YOUR ORGANIZATION PUT ITS BUSINESS CONTINUITY PLAN INTO EFFECT?

a. Yes 56.78%
b. No 4.24%
c. In Part 26.27%
d. We did not have a formal plan 12.71%

4. HAS YOUR ORGANIZATION'S RESILIENCE/BUSINESS CONTINUITY FUNCTION STRUCTURALLY CHANGED DURING THE PANDEMIC?

a. Yes 40.68%
b. No 50%
c. We do not have that function. It is baked into all the departments 9.32%

5. HAVE THE DUTIES OR RESPONSIBILITIES OF THE RESILIENCE/BUSINESS CONTINUITY TEAM CHANGED?

a. Yes 38.14%
b. No 56.9%
c. We do not have that function. It is baked into all the departments 10.17%

1. WHICH OF THE FOLLOWING BEST DESCRIBES THE PRINCIPAL INDUSTRY OF YOUR ORGANIZATION?

a. Conglomerate of Diversified Services 0%
b. Cultural Institutions 0%
c. Defense Contracting 3.51%
d. Education 4.39%
e. Engineering/Construction 1.75%
f. Entertainment & Leisure 2.63%
g. Finance & Financial Services/Insurance 20.18%
h. Government 3.51%
i. Healthcare & Pharmaceuticals 7.89%
j. Law enforcement 1.75%
k. Manufacturing 14.04%
l. Nonprofit 1.75%
m. Retail 4.39%
n. Real Estate/Property Management 0.88%
o. Security Services 9.65%
p. Telecommunications, Technology, Internet & Electronics 7.89%
q. Security Services 9.65%
r. Telecommunications, Technology, Internet & Electronics 7.89%
s. Transportation & Delivery/Logistics 4.39%
t. Utilities, Energy & Extraction 6.4%

2. WHAT IS YOUR ORGANIZATION'S ANNUAL REVENUE

a. Under $100M 11.21%
b. $100M - $500M 12.93%
c. $500M - $1B 15.52%
d. $1B - $5B 21.55%
e. $5B - $10B 6.90%
f. $10B - $20B 6.90%
g. $20B - $50B 10.34%
h. >$50B 14.66%

3. WHEN COVID ARRIVED, DID YOUR ORGANIZATION PUT ITS BUSINESS CONTINUITY PLAN INTO EFFECT?

a. Yes 56.78%
b. No 4.24%
c. In Part 26.27%
d. We did not have a formal plan 12.71%

4. HAS YOUR ORGANIZATION'S RESILIENCE/BUSINESS CONTINUITY FUNCTION STRUCTURALLY CHANGED DURING THE PANDEMIC?

a. Yes 40.68%
b. No 50%
c. We do not have that function. It is baked into all the departments 9.32%

5. HAVE THE DUTIES OR RESPONSIBILITIES OF THE RESILIENCE/BUSINESS CONTINUITY TEAM CHANGED?

a. Yes 38.14%
b. No 56.9%
c. We do not have that function. It is baked into all the departments 10.17%

6. WHAT HAS YOUR ORGANIZATION DONE WELL DURING THE PANDEMIC, WITH RESPECT TO SECURITY, BUSINESS CONTINUITY, ETC.?

Appendix II: Glossary of Key Terms

Many terms describe the process of preparing for, responding to, and recovering from a crisis or a disaster, as well as the process of maintaining operations during a crisis. Some companies use the terms interchangeably, others attach specific meanings to the terms, which may differ among companies. Below are the definitions of key terms per ASIS standards and guidelines.

Business Continuity: Ability of an organization to operate at predefined levels following a disruptive event. [ANSI/ASIS ORM.1-2017]
Business Continuity Management: Proactive set of planning, preparedness and related activities which are intended to restore an organization's critical business functions to pre-determined levels enabling the organization to operate despite serious disruptive events and recover to an operational state expeditiously. [ANSI/ASIS ORM.1-2017]

Business Continuity Plan: A collection of procedures and information which is developed, tested and maintained in preparation for use in a disruptive event to continue operations at predefined levels following the event. [ANSI/ASIS ORM.1-2017]

Crisis Management: Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capacity for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities – as well as effectively restoring operational capabilities.
Note: Crisis management also involves the management of preparedness, mitigation response, and continuity or recovery in the event of an incident – as well as management of the overall program through training, rehearsals, and reviews to ensure the preparedness, response, and continuity plans stays current and up-to-date. [ANSI/ASIS ORM.1-2017]

Crisis Management Planning: A properly funded ongoing process supported by senior management to ensure that the necessary steps are taken to identify and analyze the adverse impact of crisis events, maintain viable recovery strategies, and provide overall coordination of the organization's timely and effective response to a crisis. [ASIS GDL BC-2005]

Crisis Management Team: Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency/crisis situation and providing direction during the recovery process, both pre-and post-disruptive incident.
NOTE: The crisis management team may include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties. [ANSI/ASIS ORM.1-2017]

Disaster Recovery: Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition. [ASIS GDL BC-2005]

Organizational Resilience Management: Systematic and coordinated activities and practices through which an organization manages its operational risks, and the associated potential threats and impacts therein. [ANSI/ASIS PAP.1-2012][ANSI/ASIS SPC.4-2012]
Resilience: The adaptive capacity of an organization in a complex and changing environment.
Note 1: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.
*Note 2: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must. [*ANSI/ASIS PAP.1-2012][ANSI/ASIS PSC.1-2012 (R2017)][ANSI/ASIS/RIMS RA.1-2015][ANSI/ASIS SPC.4-2012 - with Notes] [ANSI/ASIS SCRM.1-2014 - with Notes]

Response and Recovery Plan: Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident. [ANSI/ASIS PAP.1-2012]

Response and Recovery Program: Plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations, and critical assets.
Note: Response steps generally include incident recognition, notification, assessment, declaration, plan execution, communications, and resources management. [ANSI/ASIS PAP.1-2012]

About the ASIS Foundation

The ASIS Foundation, a 501(c)(3) nonprofit affiliate of ASIS International, supports global security professionals worldwide through research and education. The Foundation commissions actionable research to advance the security profession and awards scholarships to help chapters and individuals—including those transitioning to careers in security management—achieve their professional and academic goals. Governed by a Board of Trustees, the Foundation is supported by generous donations from individuals, organizations, and ASIS chapters and councils worldwide.

Support future security research with a gift to the ASIS Foundation. Online at *www.asisfoundation.org*.