ROCK SOLID
TECHNOLOGY SOLUTIONS

BUSINESS CONTINUITY: PROTECTING YOUR BUSINESS FUTURE

An insight into the current environment and importance that business continuity has on your business reputation.

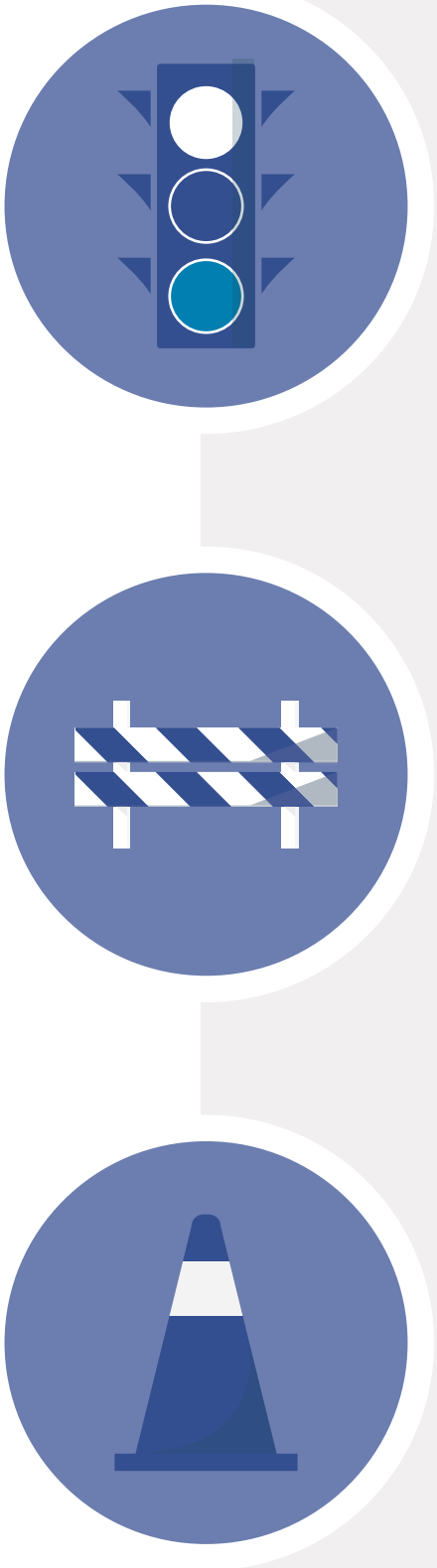
Table of Contents

Introduction

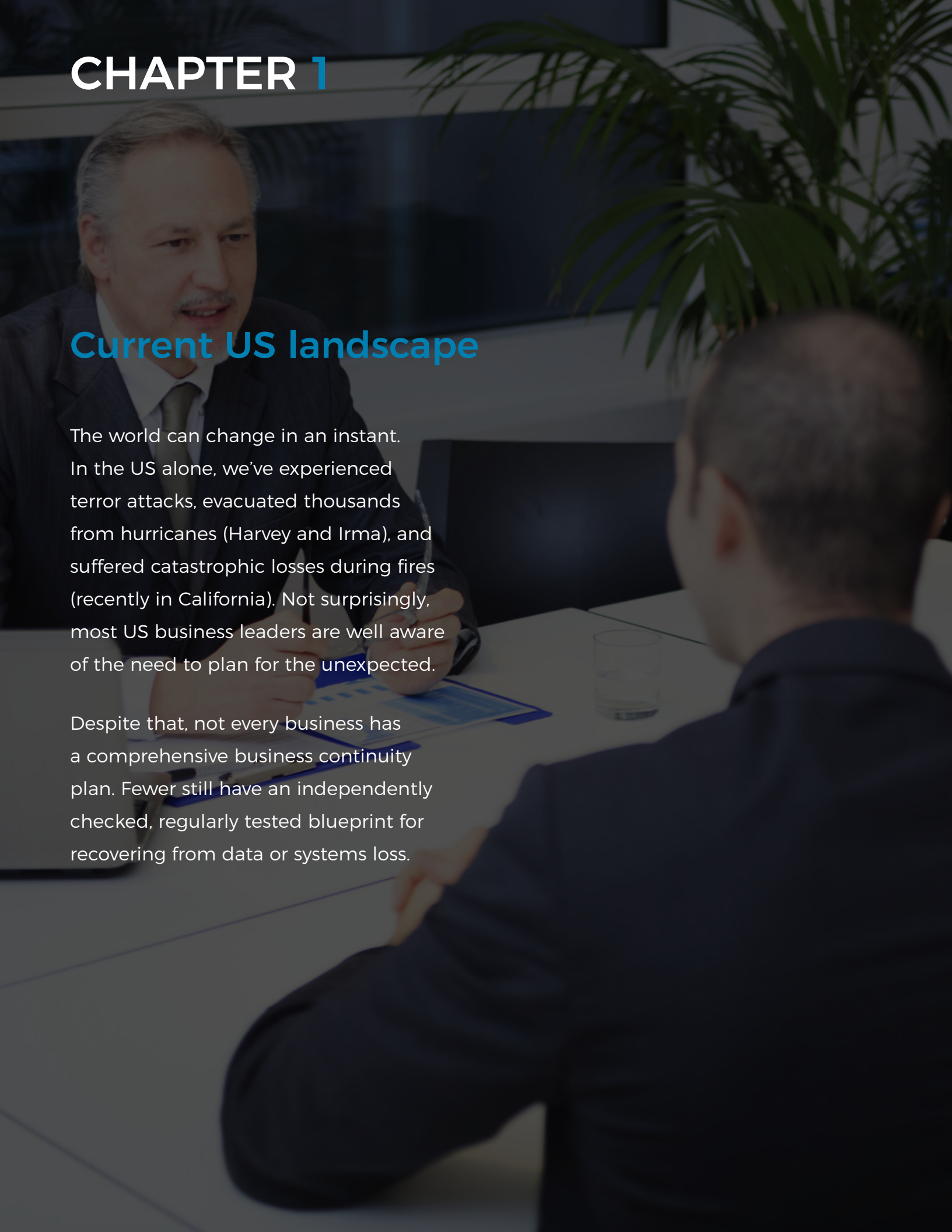
It's only natural that business leaders spend a lot of time thinking about the future. Markets are studied, products and services developed, sales forecast and production plans are carefully adjusted.

But what about the things you can't predict? Unless you're a modern-day Nostradamus, there will be bumps in the road, unexpected events that you haven't planned for. What prevents those bumps from becoming potholes?

The right business continuity plan cannot guarantee a perfectly smooth path to success – but it can prepare you to navigate safely through challenges and roadblocks.



CHAPTER 1



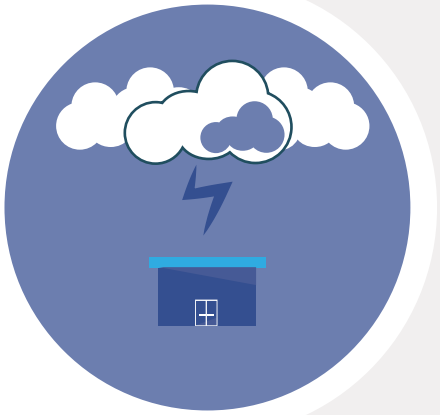
Current US landscape

The world can change in an instant. In the US alone, we've experienced terror attacks, evacuated thousands from hurricanes (Harvey and Irma), and suffered catastrophic losses during fires (recently in California). Not surprisingly, most US business leaders are well aware of the need to plan for the unexpected.

Despite that, not every business has a comprehensive business continuity plan. Fewer still have an independently checked, regularly tested blueprint for recovering from data or systems loss.

A multitude of laws and regulations specify or imply requirements for business continuity and disaster recovery planning. These requirements vary among industry sectors, affecting the development, focus and execution of business continuity plans. While banks traditionally have reasonably developed plans, this legislation, along with underlying technology and environmental trends, means that it is important to revisit business continuity strategy.

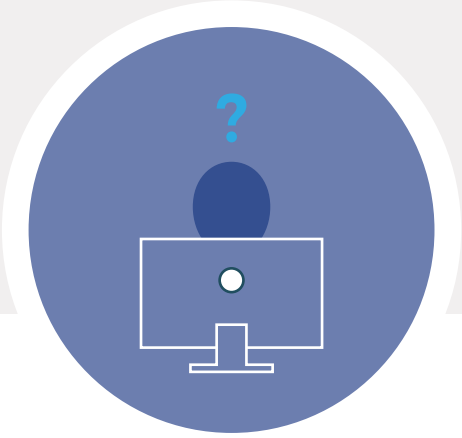
The biggest of those trends is, of course, cloud. There are significant business continuity opportunities arising from cloud models, and while US organizations are sometimes conservative in this regard, adoption is increasing. Many companies have moved their entire infrastructure to private cloud, while others have increased consumption of cloud-based applications.



Along with cloud's advantages, there are still challenges. 44.7% of business continuity professionals say securing sufficient budget reduces the effectiveness of their business continuity efforts, while 16.8 % still struggle to get top management buy-in.[1]

8 out of every 10 executives are concerned about security when storing data in the cloud.[2]

IT executives worldwide predict more than 50% of IT, customer and financial data will reside in the cloud by 2019.[2]



More than just disasters

It isn't surprising, after the United States has been tested to the limits by natural disasters, that many think of business continuity in terms of extremes. Sometimes, though, organizations are floored by the more mundane. We're talking facilities becoming unavailable or inaccessible, or human error that wipes out critical infrastructure – and who hasn't ever made a mistake at work?

Business continuity plans certainly have to accommodate nature's extremes, but they also must cover what to do when equipment failure strikes.

A new cyber threat

If all those disasters weren't enough, 2016 and 2017 have been notable for the rise in cyber-crime. Around the world, organizations have been struck by attacks (e.g WannaCry, Petya, NotPetya) increasingly in the form of ransomware that prevents access to systems.

Across the globe, an estimated 5% of small-to-mid-sized businesses (SMB's) fell victim to ransomware from 2016-2017.[5]

32% of organizations admitted being affected by cyber-crime.[3]

34% expect to be affected by cyber-crime in the next 2 years.[3] Just 37% of organizations have a cyber incident response plan.[3]

THE COST OF CYBERCRIME IN THE UNITED STATES OF AMERICA

TOTAL RANSOM PAID BY SMBs TO RANSOMWARE HACKERS Between Q2 2016 and Q2 2017

$301 MILLLION (USD)

The ransom requested is TYPICALLY between

$500 AND **$2,000**

Ransomware virus remained on an smb's system after the first attack and struck again at a later time

29% **OF MILLENIALS**

Report Loss of Data and/or Devices

57% **OF MILLENIALS**

Report Business-Threatening Downtime

75% **OF MILLENIALS**

CHAPTER 2

BC vs DR

You may have heard the terms 'business continuity' (BC) and 'disaster recovery' (DR) used seemingly interchangeably, but there are some important differences.

A disaster recovery plan covers in detail how business applications are to be recovered in the event of a crisis. It prepares the IT team to recover essential services. For this reason, a DR plan may examine backup methods, outline a damage assessment process, and evaluate how the incident response time can be improved.

BC planning looks at the bigger picture. It answers the question, 'how would the business continue to operate if we lost other dependencies such as building, utilities, staff, or suppliers?'

43%

of companies never reopen after a major loss of business data.

51%

close within 2 years.

6%

survive long-term.[4]

BC vs DR continued...

Your BC plan should include your recovery priorities in order to keep providing key products or services. It will make sure your people are ready to do whatever is needed to ensure your customers are taken care of. In addition, a BC plan typically makes sure you can work with suppliers and business partners to fulfill and deliver orders without missing important commitments.

The two plans – disaster recovery and business continuity – not surprisingly interconnect. In a world where IT systems and applications play such a key business role, most well-prepared organizations turn to their trusted technology partner to help develop solid plans.

Protecting your business reputation

In almost every transaction, your customers trust you with important data. They also expect a level of service and availability consistent with your brand. A good brand adds value to your business beyond the physical – and its value is hard to fully measure.

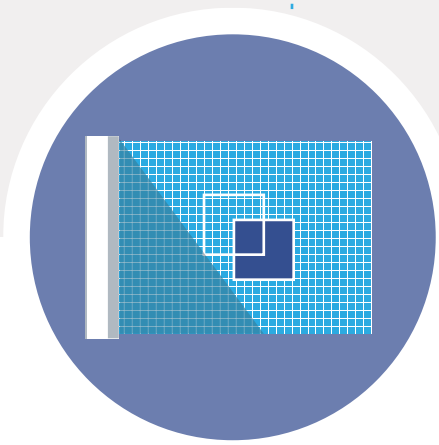
Suffice to say, the old customer service rule of thumb should be expanded to suit the social media age: provide good service, and your customer may tell a person or two. Provide good service, and your customer is every possibility of it going viral. How you deal with crises is the difference between winning new admirers and finding your customers leaving in droves.

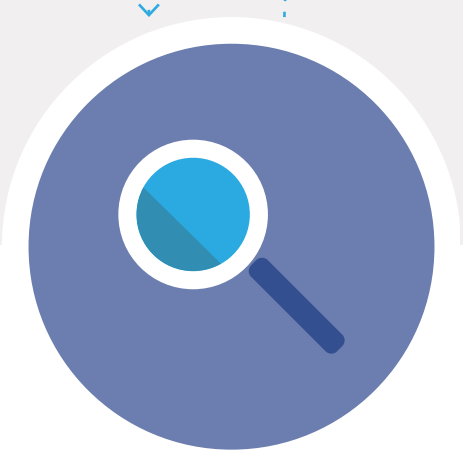
Protecting your reputation must be a key priority in a business continuity plan – which means it must extend beyond the IT department. Board members, senior management and public relations staff; sales and customer service personnel; and key team members in logistics must be prepared to act to ensure customers are supported.

CHAPTER 3

The six steps to securing your business future

Creating a business continuity plan means understanding the organization in detail. For a business continuity specialist, this means spending time with people in all kinds of roles. Working closely with all levels of your business, they work through six key steps to make sure your business stays on track through any crisis.





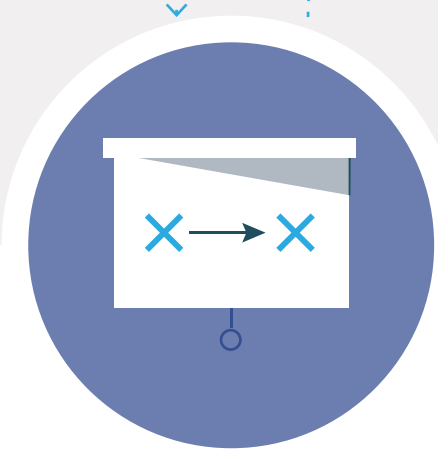
1 Program design.

In this stage, expectations are clarified, senior management are engaged, and planners make sure the blueprint aligns with the needs of the business. During the design phase, it is important to make sure that the right resources and support are available.

2 Business impact assessment (BIA) & risk assessment.

This phase involves a detailed study of business activities. It explores the dependencies required to deliver products and services. At the end of this stage, the planner must understand exactly how critical products and services are delivered, from supply, through production and packing, to dispatch and invoicing. This phase is critical to ensure the BC plan has strong foundations.

In this phase, an IT strategic roadmap is invaluable. The roadmap will provide documentation of all key systems, outlining interdependencies. It will include diagrams of the entire architecture, information about any issues, as well as a systems inventory. This information is vital in your BC plan, so maintaining a current IT strategic roadmap is a key element of IT management best practice.



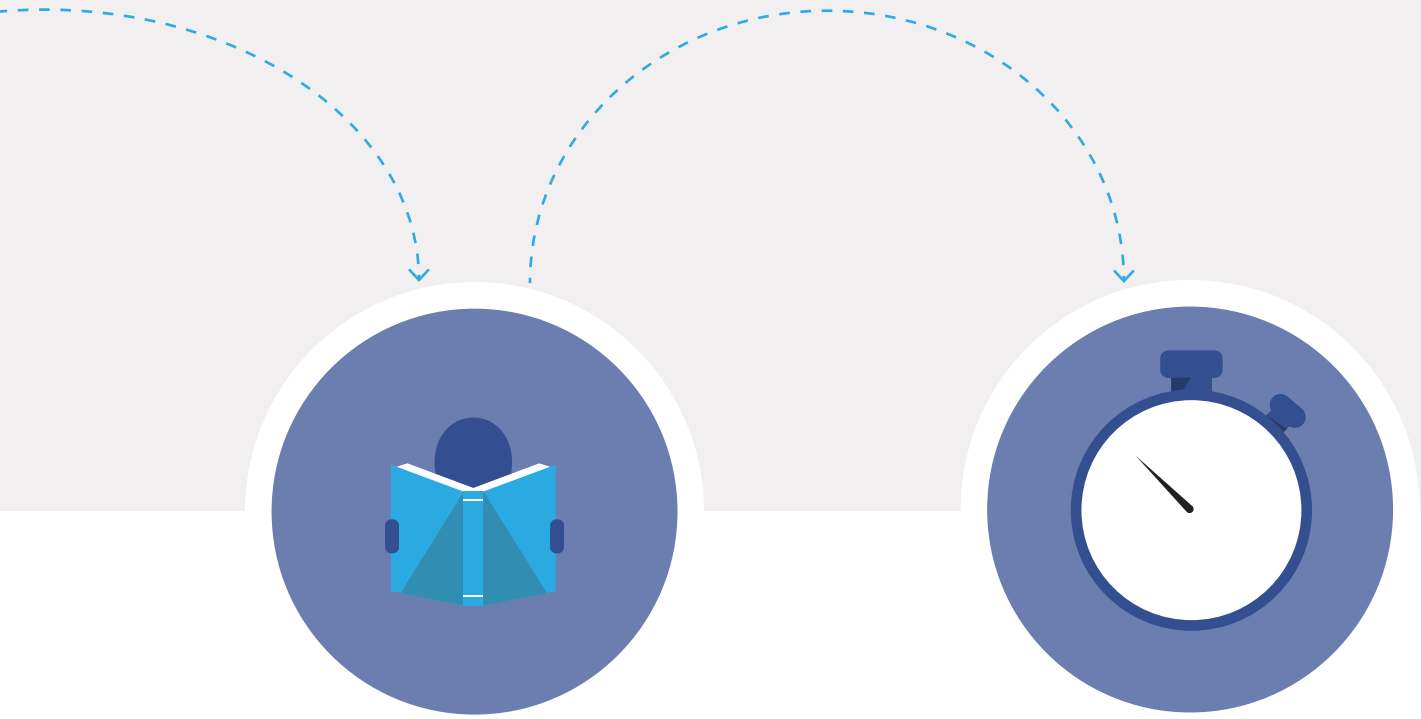
3 Strategy development.

Armed with the information gathered in the BIA, the business can begin to identify possible ways to mitigate risk. The recommendations from this phase can be assessed for cost, customer impact, available resources, and how well they sit with the organization's risk profile.

4 Plan development.

The BC plan is the document that guides your business through any disruption, be it natural disaster, cyber-crime, or road-workers digging through power cables. It will include a crisis management plan to guide senior management, along with a crisis communication plan for anyone dealing with public or media inquiries. This might include prepared statements and messaging.

The overall BC plan will also include the IT disaster recovery plan, to recover core technology assets within an agreed timeframe. Completing the set is a business recovery plan that includes the complete recovery of all key business activities, so that important products and services are available exactly as your customers expect.



5 Training and awareness.

A business continuity plan can only work if everyone knows where it is, what it is, and what part they play. In an emergency, when emotions run high, panic can set in. This is not the best time to be making important decisions about your business.

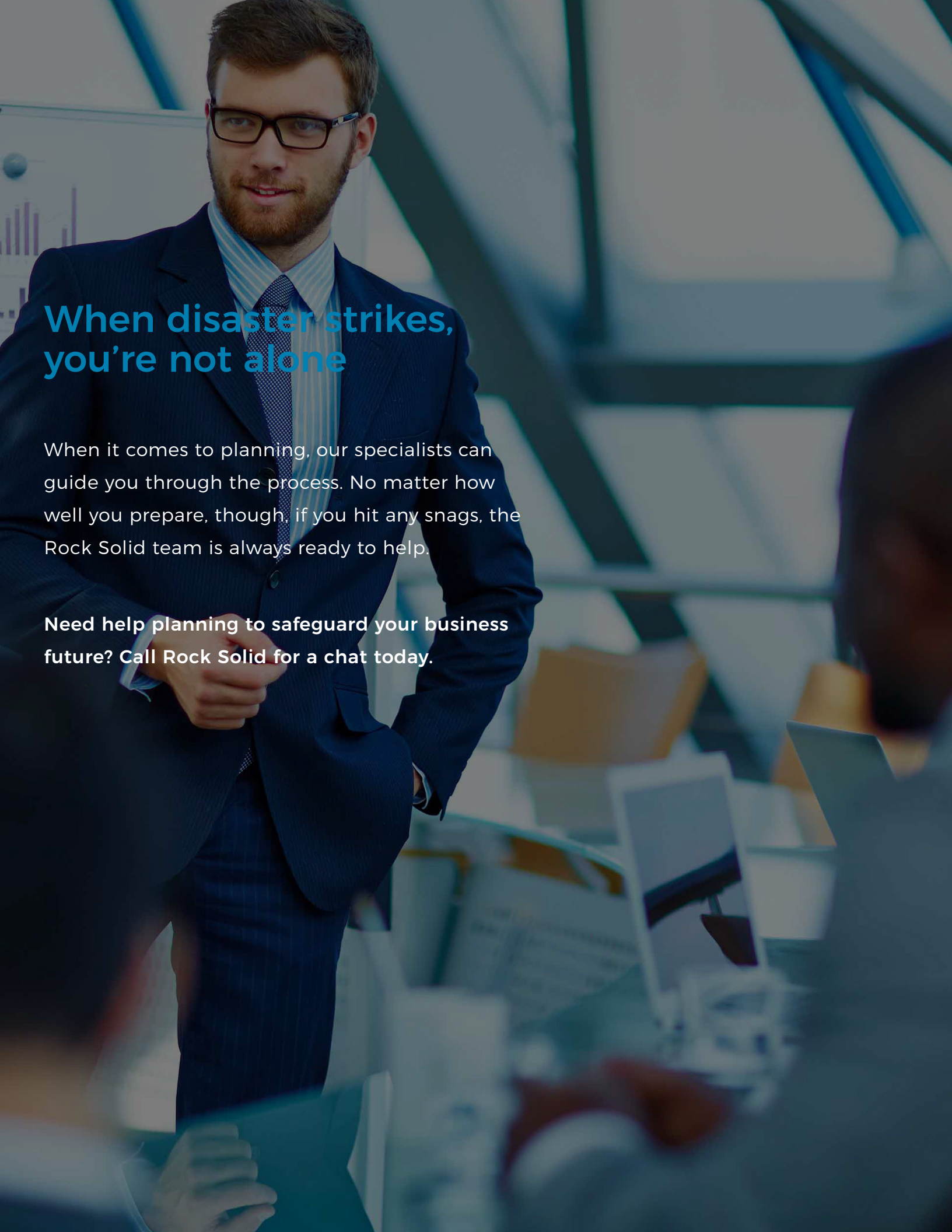
For this reason, your training plan is very important – business continuity training can be the difference between survival and failure. Everyone from senior executives to new production hires must be included – so involving human resources in making the BC plan part of induction training is a good idea.

6 Exercise and review.

When individuals have practiced a plan, they are far more likely to take the correct actions: they will know exactly what to do. Your BC plan should not be restricted to an academic exercise – instead, involve the business in simulations of actual emergencies.

This gives you a chance to see what works, and what doesn't. The plan can be updated accordingly.

From a human perspective, people are far more likely to act on emergency training if it is rehearsed, so that the right decisions become automatic. If it means bribing colleagues with take-out and drinks to stay late and practice, it is worth it. After all, it is a small cost to pay to meet customer expectations when disaster strikes.



When disaster strikes, you're not alone

When it comes to planning, our specialists can guide you through the process. No matter how well you prepare, though, if you hit any snags, the Rock Solid team is always ready to help.

Need help planning to safeguard your business future? Call Rock Solid for a chat today.

ROCK SOLID
TECHNOLOGY SOLUTIONS

About Rock Solid Technology

Every moment lost to technology trouble is a missed opportunity to move your business forward. Don't take a chance when it comes to your company and leave the IT to the professionals.

Outsourcing your IT department to the experts at Rock Solid Technology Solutions protects you from unexpected troubles and unreliable systems. We create innovative, yet effective solutions to help your business run smoothly.

By working with RS Technology, even small companies can cost-effectively leverage extensive technology experience. We keep up with the developments in technology, so you can do what you do best.

Contact Us

Rock Solid Technology Solutions

1000 Business Center Circle, Suite 221
Thousand Oaks, CA 91320
Phone: 818-483-0802
Fax: 818-475-5267
Emergency Support: 800-608-4693
www.rstechnology.net

REFERENCES

1 ContinuityCentral.com
2 Teradata
3 19th Annual CEO Survey
4 IBM 2011
5 Datto's State of the Channel Ransomware Report, Oct 2017