The Ultimate Guide to

Business Continuity

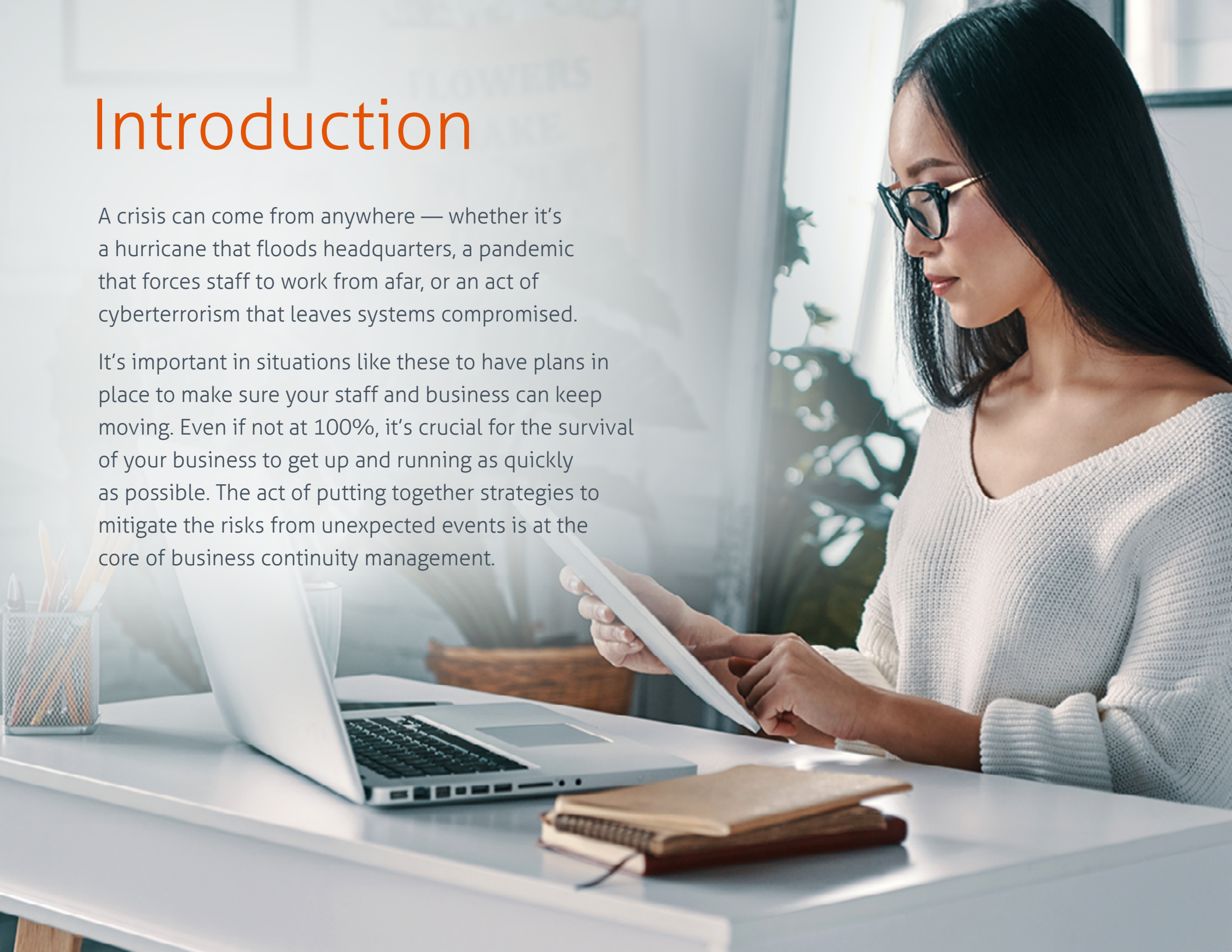
Laserfiche®

Contents

Introduction

A crisis can come from anywhere — whether it's a hurricane that floods headquarters, a pandemic that forces staff to work from afar, or an act of cyberterrorism that leaves systems compromised.

It's important in situations like these to have plans in place to make sure your staff and business can keep moving. Even if not at 100%, it's crucial for the survival of your business to get up and running as quickly as possible. The act of putting together strategies to mitigate the risks from unexpected events is at the core of business continuity management.



Chapter 1

Business Continuity at a Glance

If you want to take a comprehensive approach to business continuity management, you should create the following:

Risk Assessment

This involves identifying potential threats to your business or processes. Nothing is off the table, and your list may include anything from burglary, to blizzards or even a military conflict. If you identify a threat that could potentially impact your day-to-day, put it on the list.

Business Impact Analysis (BIA)

This should be a list of impacts to your business, such as a loss of income, productivity or even your business's reputation. You should create a BIA for each of your critical processes and systems.

Disaster Recovery Plan (DRP)

Primarily a concern for your IT department, DRPs are plans to recover data, systems and applications. You can and should create separate DRPs for each critical system and application.

Business Continuity Plan (BCP)

These plans should be in place to ensure that a business process can continue, even if you don't have the people, workflows or resources you would under normal circumstances.

Crisis Management Strategy

This largely deals with the human side of the crisis. How do you ensure staff safety? Who talks to your vendors, customers, internal stakeholders and the media? What do they say?

Chapter 2

Risk Assessment

A risk assessment is all about identifying the threats to your business and its processes, wherever they might originate.

For example, if a flood wipes out a financial firm's records and they don't have a backup site (or the backup site is too close by and also flooded) the compliance issues from destroyed records will linger for months or even years afterward.

Whether the disaster is natural or man-made, it's important to identify and plan for situations where you may not have access to the data, resources or staff you're accustomed to during normal business operations.

According to Business News Daily, these are the most common mistakes firms make when it comes to business continuity management:

- Not accounting for loss of critical people nor planning for the stress and trauma of staff.
- Not making the emergency plan accessible to staff at the office or working remotely, or making plans that are too generic, too detailed or too stale.
- Failing to address communication choke points and having PR issues related to recovery.
- No alternative emergency operations center (EOC) or recovery sites, or not having a plan for employees to work from home when a physical site isn't available.
- Believing that outside assistance and insurance will take care of everything.

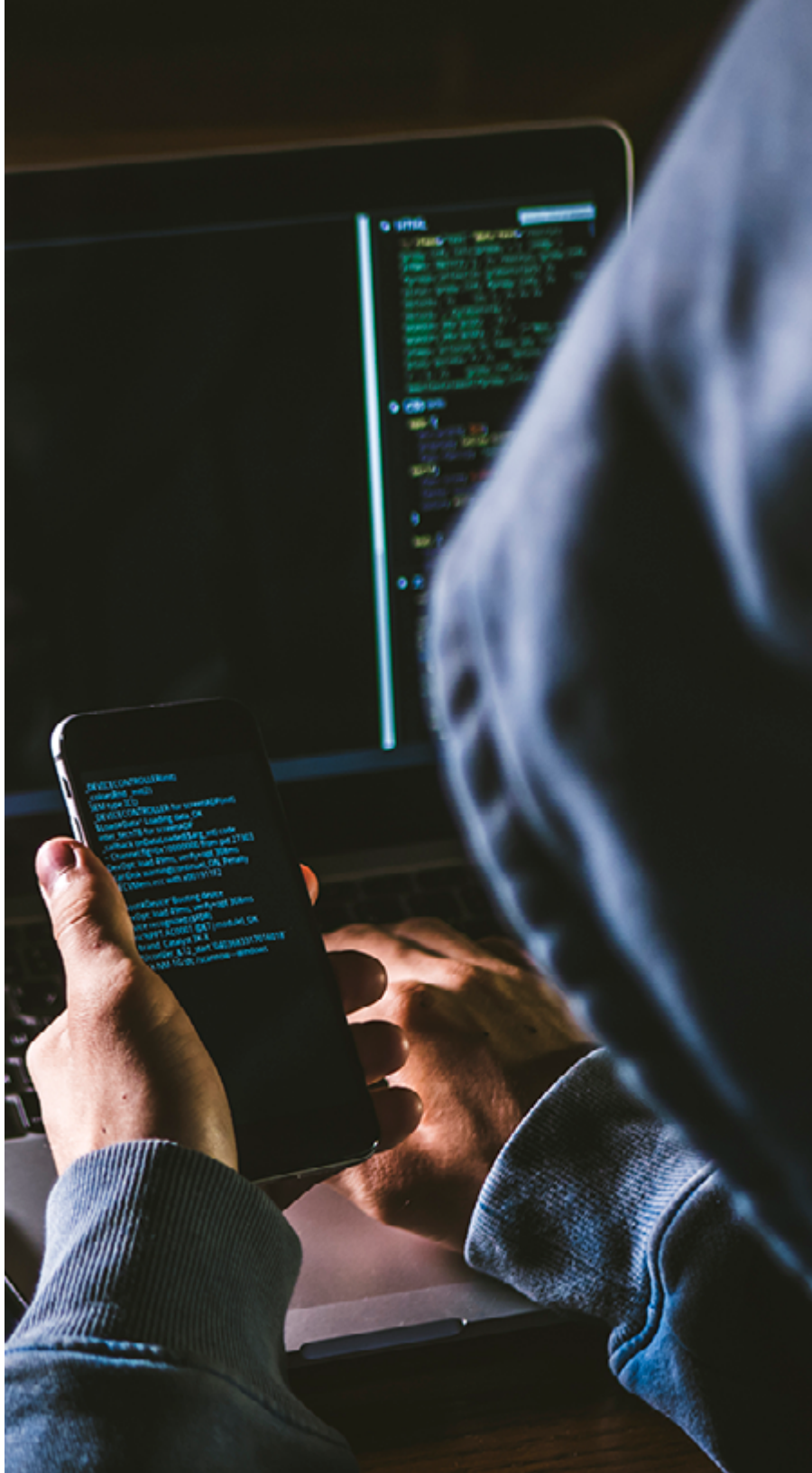
The only way to truly avoid these mistakes is to become a master in the art of expecting the unexpected. Although sources for business disruption can be numerous, most disasters fall into four common categories that you should be aware of when performing a risk assessment:

Scenario 1: Loss of Systems And Data

Businesses should always be aware of risks to their systems, networks and data. It's not just natural disasters that could lead to a loss of these items either. Property crime and cybersecurity breaches are also significant factors.

In the highly regulated healthcare industry, a data breach means affected individuals, media outlets and the U.S. Department of Health and Human Services have to be notified right away. Your recovery plans need to account for these types of regulations.

As far as data backups, you really need to think big. Multiple data centers strategically placed in different regions, and a focus on cloud-based solutions are just a few of the ways you can ensure your data and systems recover and with minimal data loss.



Scenario 2: Loss of a Building

Business continuity plans should account for scenarios involving the loss of a building. This can include cases where:

- The office was damaged in a fire.
- A nearby chemical spill creates a health risk in the area.
- An active crime scene is at the office or across the street.
- Citizen protests (or in more extreme cases, riots) block city streets and could risk employee safety.

Recovery plans should include plans for alternate work sites. Ideally, with the technology resources available to both businesses and consumers, a work from home situation might be easier for your employees and more cost effective for the business. In either case, employees should have the ability to remotely access applications, systems and data securely during a disaster event.

Scenario 3: Loss of Third Party

For today's fast-moving organizations, many rely on third-party services within their departments, including payroll, IT, digital marketing and HR. Recovery plans should account for third parties that may go bankrupt or abruptly stop providing key services. Businesses should identify a list of alternate providers prior to a disaster, and a plan to migrate data to the alternate service, to minimize their reliance on any single vendor.

Scenario 4: Loss of People

The loss of key employees significantly impacts any business — especially if individuals are not cross trained on essential responsibilities. As part of their continuity strategy, businesses need to train staff so they can backup each other's responsibilities and perform critical processes in a crisis.

When exploring your own business continuity management, it may seem like you have to account for everything. This is particularly troubling when you consider "black swan" events: you don't know if an earthquake will cause a tsunami, or if a virus outbreak in one country will become a pandemic that affects the world. The best you can do, and what you should do, is consider the broader scenarios above to account for all the ways that any disaster, regardless of its source, can affect your business. Focus on what you can control, and you'll be able to prepare for unexpected events that you can't.

Chapter 3

Business Impact Analysis

Once you've identified the threats your business can face, it's time to perform a business impact analysis, or BIA. This process involves:

- Identifying processes affected by particular events.
- Identifying the type of loss (financial, productivity, reputation.)
- Quantifying the level of potential loss.
- Setting a recovery point objective (RPO) that specifies a maximum acceptable amount of data loss in a disruption.
- Setting a recovery time objective (RTO) that specifies a maximum acceptable amount of time a system or process can be down.

Example: Online Retail

Your online retail site has recently become a victim to a DDoS (Distributed Denial of Service) attack. While you're working to recover, what type of losses might you experience?

Type of loss:

Financial

Loss of revenue from customers that made orders that weren't backed up and thus not fulfilled, and those that could have made orders but couldn't access the site.

Reputation

Customers dissatisfied that they can't order items, or simply don't receive them if their order was part of a loss of data.

Quantifying impact:

RPO

Data from purchases should be backed up instantly, especially since money is involved. If current data on purchases is even remotely out of date, this can cause significant disruption across the business.

RTO

Ideally would like to recover in seconds, however if the site is down for more than fifteen minutes, the business can lose significant revenue.

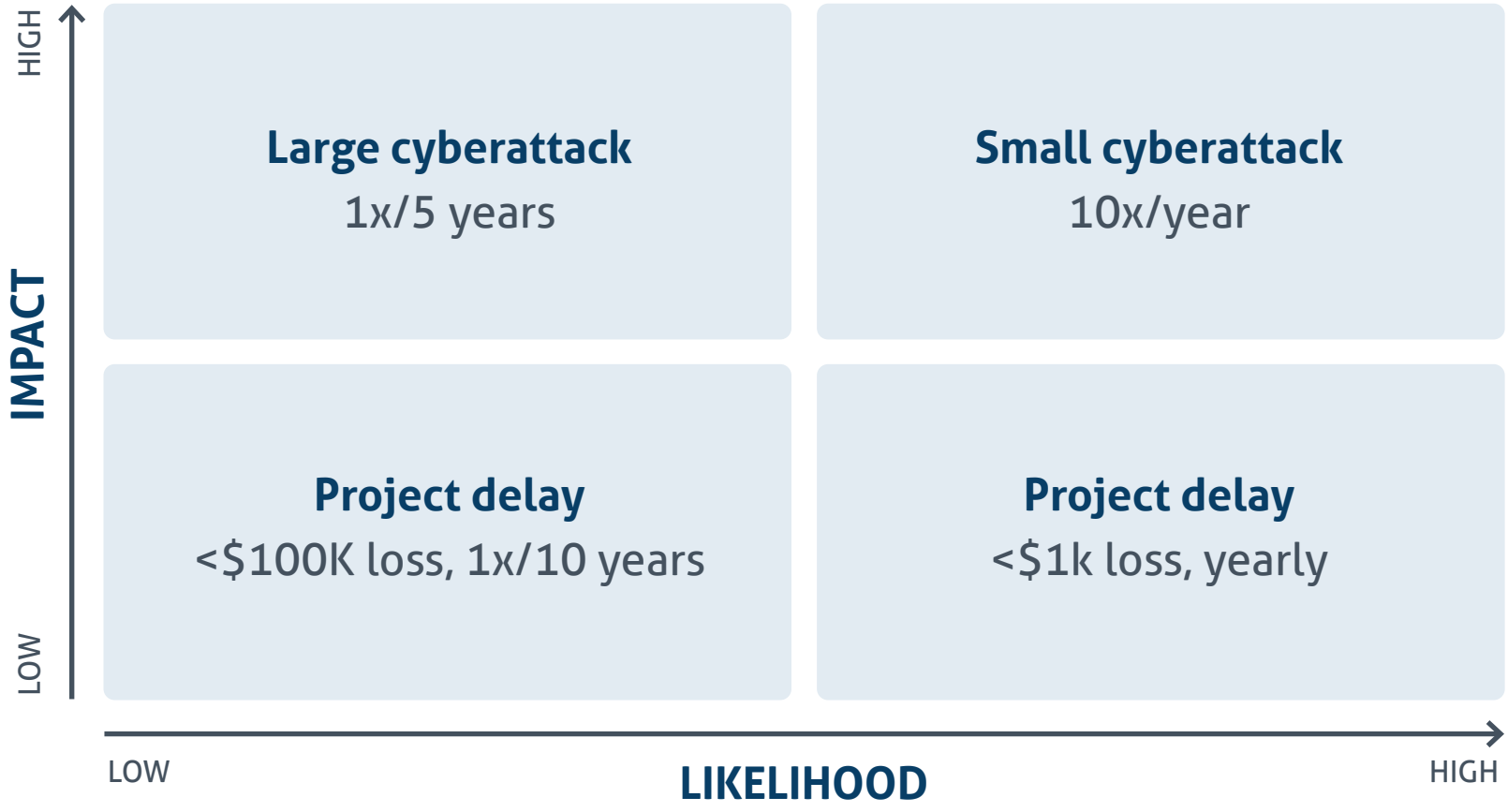
Level of loss

If RPO and RTO thresholds aren't met, the business could lose over an estimated $1M USD in revenue and a reputation that might take approximately a full year to recover.

Chapter 4

Managing Priorities

If the pursuit of perfection keeps you from seeing the forest from the trees, your business could be in serious trouble. One way you can prioritize within your business continuity management strategy is to create a chart like the one seen below, as popularized by IT governance association, ISACA.



Note that the quadrants sort business impacts into four distinct categories:

Low impact/low likelihood

Some project delays are inevitable for most businesses. Even with potential loss revenues, if it's infrequent, your tolerance for such losses can be quite high.

High impact/low likelihood

A large scale cyberattack can cause devastating effects to any business. Although improbable, you want to ensure business is ready for this kind of event.

Low impact/high likelihood

Project delays can be low impact on their own, but if they're frequent these small disruptions can add up to big losses in the long run.

High impact/high likelihood

Smaller scale cyberattacks can still cause devastating effects on their own, and can happen more frequently. You'll want to bolster your IT infrastructure against these attacks.

Chapter 5

Disaster Recovery

Disaster recovery primarily revolves around making detailed plans to recover your systems, data and applications. While conducting an internal audit or having one conducted by a third party, your plan should account for:

- Your geographic location
- Nature of your business
- Any legal or regulatory frameworks

Example: Finance

Let's say you're a finance firm located in Los Angeles. Finance is a strictly regulated industry, and firms are required to maintain records in a very specific manner. Also, since the firm is in LA, you're at an elevated risk for earthquakes.

Given these constraints, you'll want to ensure that your data centers are backed up (to avoid fines if a data center is destroyed) and that your back up centers are located in other locations (a backup data center in Wyoming, for example, might be less susceptible to earthquakes.)

Chapter 6

RPO and RTO

While the parameters of your RPO and RTO should be outlined in your BIA, how you go about meeting them should be a part of your plan.

As strategies will inevitably differ in the amount of time they take to implement, it's important to consider what strategies can work within the timeframes set by your RPO and RTO.

As seen in the chart below, keeping multiple instances of your service running (active-active clustering) is one of the fastest strategies, as if one instance of your service goes down, the other is already active. The slowest measure would be a system you have to activate manually as a backup (also known as a cold standby.)

In terms of RPO, real-time replication of your data (a common feature among today's cloud solutions) can likely restore data from seconds ago, while a snapshot may be too out-of-date to meet your requirements set out in your RPO.

Chapter 7

Business Continuity Planning

At the core of a business continuity plan is having steps you can follow to continue a particular business process in the event it's disrupted. Business continuity plans can and should be created for disruptions of all levels, from a disruption to your marketing automation platform, to situations where your building is inaccessible.

Example: Payroll

An obvious critical need of any business is to pay its employees, and on time. What if your accounting department can't access your electronic payroll system? Your business continuity plan should outline the process:

- Get last period's payroll numbers.
- Confirm with management any changes since last period.
- Write and issue checks to employees based on these numbers.
- Work with bank to arrange automatic transfers based on these numbers until system is restored.

If the process should only be disrupted for a short time, should you start writing checks anyway? While this ultimately is up to the discretion of your business, it may be a good idea to set an RTO for when you should resort to using a manual process.

Chapter 8

Crisis Management

Crisis management is primarily about making executive decisions, those that calmly ensure command and control over the chaos that pervades a crisis. This involves managing employee safety and well being, as well as developing a strategy to communicate with those inside and outside the company. Part of your crisis management strategy may include:

- Creating a crisis management team to form and enact executive decisions in a crisis.
- Drafting a checklist the team can use to ensure all their bases are covered.
- Developing a public relations and internal communications strategy.

Case study: BP Oil Spill

In 2010, British Petroleum was facing a serious crisis after an explosion on one of their oil rigs killed 11 workers and caused one of the worst oil spills to hit the shores of the United States. While as many as 3 million liters of oil per day were spilling into the Gulf off the shores of Louisiana, CEO Tony Hayward simply said he wanted "his life back," seemingly ignoring the plight of those in Louisiana, and the tragic deaths of his own workers. These remarks, as well as continual attempts to downplay the severity of the accident and its environmental impacts, brought significant criticism.

Although there is still reputational damage to this day, the company nonetheless took steps – that could have been taken much earlier – to take control of the crisis. First, they enlisted Glenn DaGian, a former BP employee who had been notably critical about the incident, as well as a Louisiana native, to assure locals they're working to resolve the situation. Choosing someone who understands the local culture of the affected communities helped the firm get a better understanding of the social impact of the disaster.

As far as communication strategies, Hayward was replaced by Mississippi native Bob Dudley. The company also quickly engaged social media to communicate directly with the public – not to apologize, as their former CEO had done, but to give updates and thus some peace of mind to those watching that they're taking control of the situation as best they can. It also gave a platform for the public to vent their frustrations. To BP consultant Steve Marino, who helped lead social media efforts, the social media platforms "allow[ed] people to feel that BP was hearing them, which they were."

Although it's clear BP likely didn't have a checklist or a formal management strategy for this type of crisis, their initial failures, and attempts to learn from them, show how important it is to have a plan in place to find the right people and right messaging to manage a crisis effectively.

Chapter 9

Plan Testing

Even if you'd laid out a comprehensive plan, you really don't know if it's up to the task until you try it out. It's important that you test your plans, especially those that have a high impact on your business. The goal of any of your tests should be:

- Verify your BCP is accurate.
- Gauge staff performance in this type of situation.
- Evaluate coordinating among team members and external parties.
- Measure the performance and capacity of backup sites in a simulation of the event.

Example: Global pandemic

In a case where a new, highly-contagious disease is spreading, you may need to close down your office to stop the spread, or even forced to by governments as they enact their own measures to stop the contagion. In such cases you'll likely want employees to work from home. To test this strategy, you could have employees work from home for a day to evaluate the plan based on your goals:

Verify your BCP is accurate.
Does having your staff work from home address the event?

Gauge staff performance in this type of situation.
Do they have the resources they need to perform essential job duties?

Evaluate coordinating among team members and external parties.
Can employees still communicate and conduct meetings? Would you be able to effectively communicate with vendors, customers or the media?

Measure the performance and capacity of backup sites in a simulation of the event.
Can you meet your RPO and RTO in the event of a disruption to your applications, services and data?

In addition to your own audits and tests, you may want or need to have your plans audited by a third party. Common standards your business continuity plan might need to comply with include ISO Standard 22301, NFPA 1600 and ISACA CISA IT Governance Domain 2. The goals of these auditors are usually to:

- Understand the connection between a BCP and business objectives.
- Determine whether the current BCP is sufficient and up-to-date.
- Review plan testing to verify the proposed effectiveness of the BCP.
- Visit or evaluate offsite or cloud-based storage.
- Assess staff's ability to respond affectively to a crisis event.

One you've tested out a plan, it doesn't mean that you're done. Developing and testing business continuity and disaster recovery plans are iterative processes — they're always evolving and there's always an opportunity to revisit your strategy.

Chapter 10

ECM + Cloud as a Part of Your Organization's Business Continuity Plan

Organizations managing their content on the cloud are at a distinct advantage during a disaster. With enterprise content management (ECM) — software designed to digitally manage content and processes across the enterprise — they can continue operations under the most disruptive circumstances. Ensuring that staff can access their work anytime and anywhere is more than just a convenience — it can be a lifeline for organizations during uncertain times.

Having an ECM system as part of your business continuity plan is a way for you to quickly respond to disasters and interruptions by:

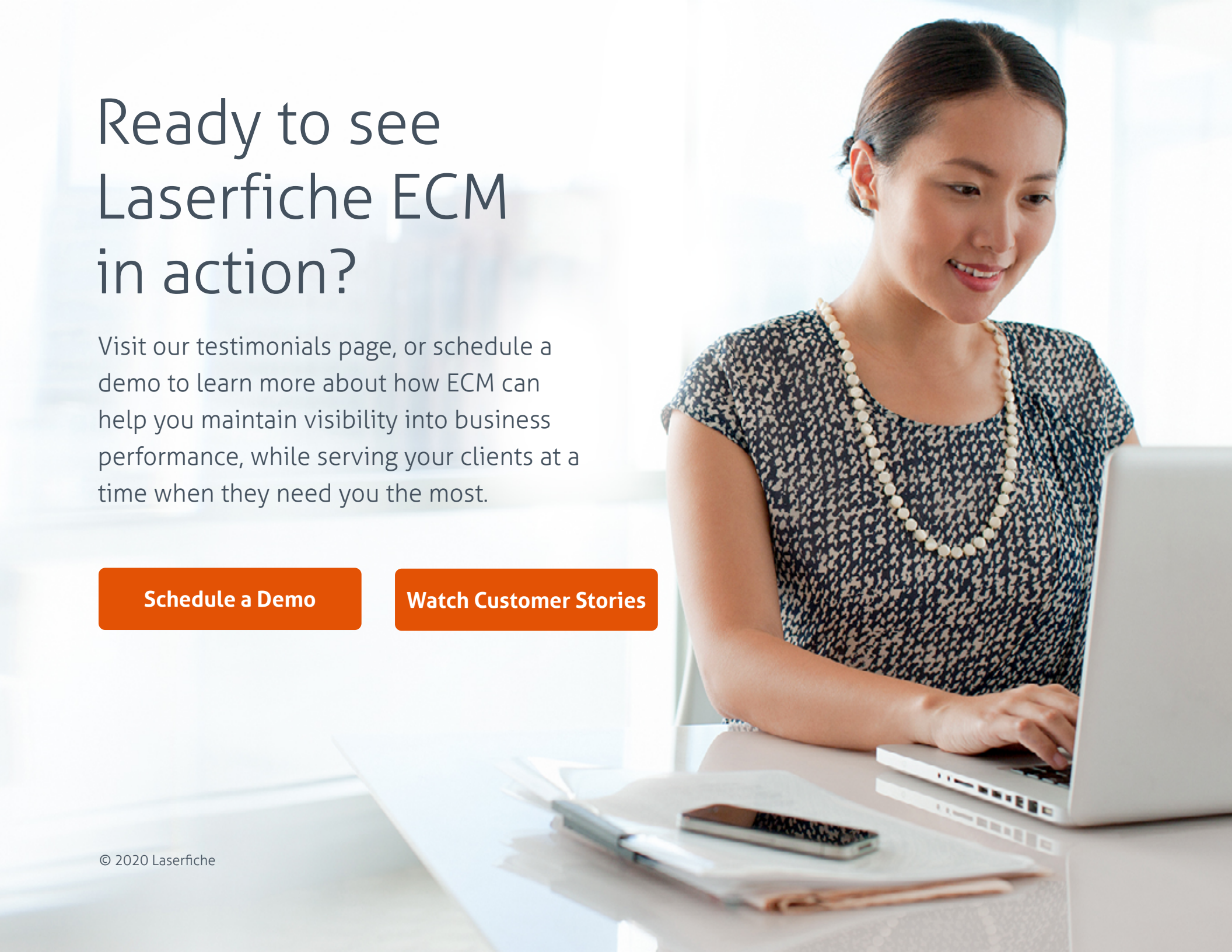
- **Enabling a digital workplace with cloud technology**, giving employees access to information, systems and processes they need to perform their job functions and ensure business keeps moving.
- **Giving staff collaborative document editing and version control features** so they can work together on the most current and up-to-date versions of documents.
- **Offering online services to clients, customers and vendors** so they have all the information they need even if your physical office is closed.
- **Automating critical processes that ensure standardization, consistency and continuity**, giving employees peace of mind that things are still running smoothly.

Ready to see Laserfiche ECM in action?

Visit our testimonials page, or schedule a demo to learn more about how ECM can help you maintain visibility into business performance, while serving your clients at a time when they need you the most.

Schedule a Demo

Watch Customer Stories



About Laserfiche

Laserfiche is the leading global provider of intelligent content management and business process automation. Through powerful workflows, electronic forms, document management and analytics, the Laserfiche® platform eliminates manual processes and automates repetitive tasks, accelerating how business gets done.

Laserfiche pioneered the paperless office with enterprise content management more than 30 years ago. Today, Laserfiche is innovating with cloud, machine learning and AI to enable organizations in more than 80 countries to transform into digital businesses. Customers in every industry — including government, education, financial services and manufacturing — use Laserfiche to boost productivity, scale their business and deliver digital-first customer experiences.

Laserfiche employees in offices around the world are committed to the company's vision of empowering customers and inspiring people to reimagine how technology can transform lives.

Connect with Laserfiche:

Laserfiche®