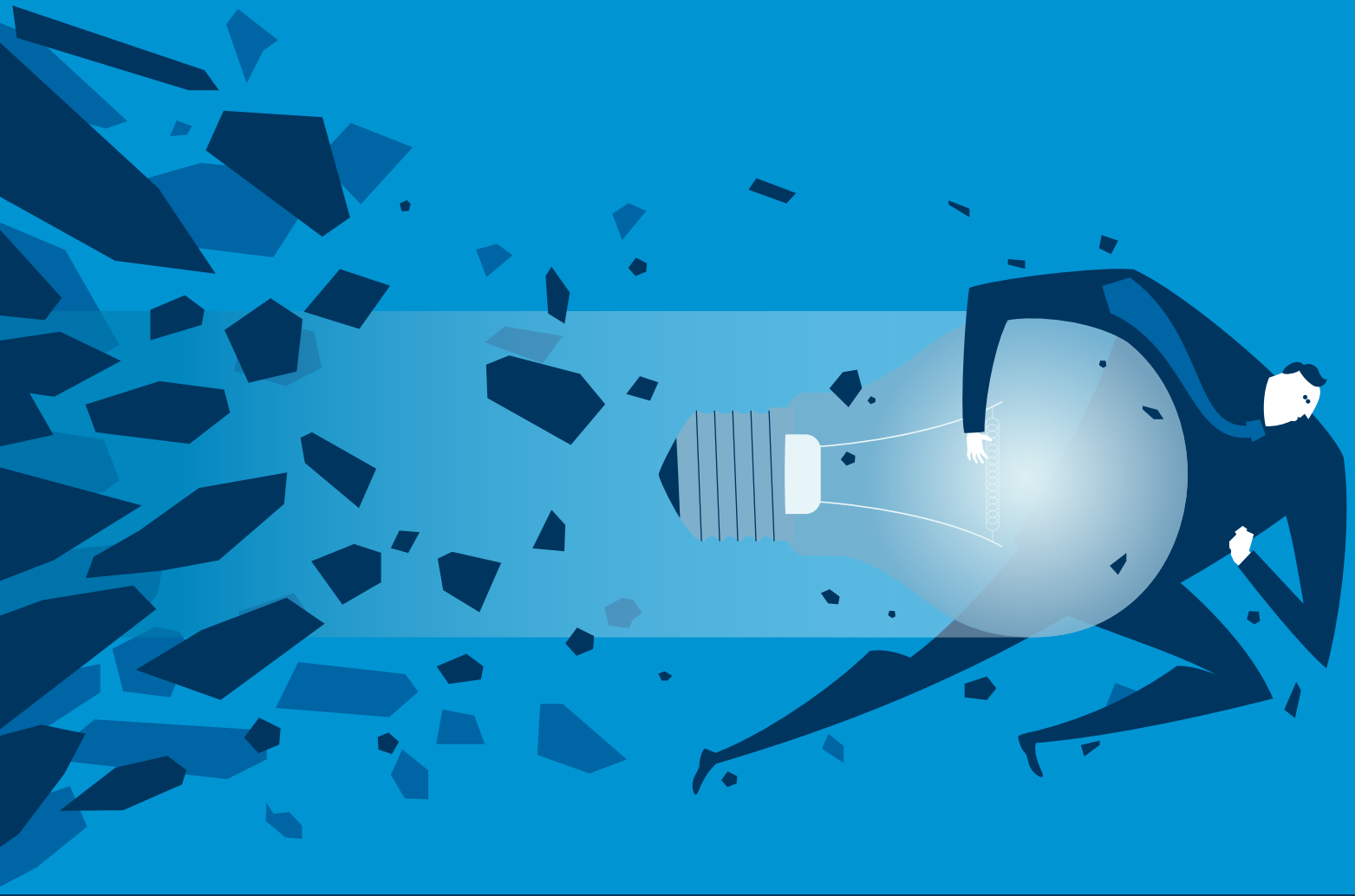
THE ULTIMATE GUIDE TO

BUSINESS CONTINUITY PLANNING



WHAT'S INSIDE?

Disasters you need to prepare for

Why disaster recovery isn't enough

Strategies for developing a business continuity plan of your own

PLUS much, much more!

Laserfiche®
Run Smarter®

www.laserfiche.com

WHAT'S INSIDE

Introduction

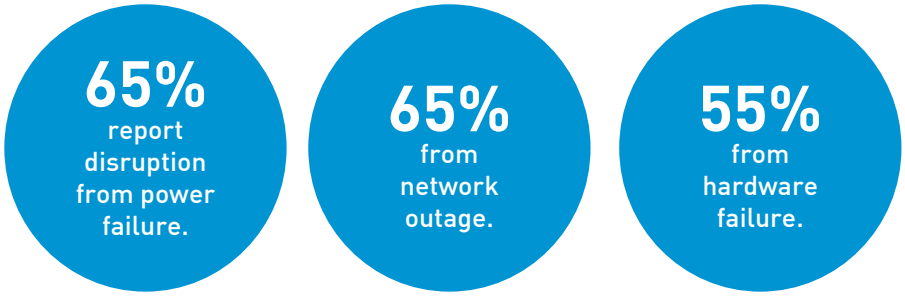
ESG, a consultancy group focused on storage and information management, found that 63% of organizations could withstand only four hours or less of downtime before experiencing adverse affects to the business. Depending on the organization and industry, the time to get critical applications up and running after an outage has decreased from hours to minutes—or even seconds.

Business continuity planning is the solution to mitigating the impact of a disaster, no matter its source. Industry estimates show that **40% of organizations without business continuity and recovery plans will go out of business within a few years of a major disaster.** In fact, the Institute for Business and Home Safety, an insurance industry trade group, estimated that **25% of businesses that close during a disaster will not re-open.**

Beyond Catastrophic Disaster

Defining what a disaster actually is has become crucial as organizations shift their perception of disaster. When you think of a "disaster," natural disasters like floods, fires or earthquakes immediately spring to mind. But it isn't just catastrophic disasters that you need to plan for...

A recent IDG Research study showed that 92% of respondents have encountered at least one disruption to their business systems. While high-profile events like hurricanes, earthquakes and terrorism get attention, they serve as distractions from the real threats:



Focusing on natural disasters and terrorism diverts attention from the realities of today's business environment and the deteriorating state of IT infrastructure.

"Our major electronic workflows could halt production if they stopped working properly," says Michael Eklund, Information Systems Coordinator at RMS, a contract manufacturing company that specializes in medical device implants and surgical instruments. "Because of that, we look for reliable technology that's easy to implement, administer and use."

The Periodic Table of Disasters A ··· TO ··· Z

AW acts of war						
A arson	Bl blackouts					
Bz blizzards	BT bomb threats	Br bribery	BC bridge collapse	BF brush fires	CA chemical accidents	CD civil disobedience
CF communications failure	Ca cyber-attack	D disease	DE disgruntled employees			
E earthquakes	Em embezzlement	Ex explosion	F fires			
Fl floods	HC hardware crash	HW high winds	HS hostage situations	H hurricanes	IS ice storms	K kidnapping
MO military operations	M mudslides	NF network failure	LD labor disputes	L lightning	PC plane crashes	
RA railroad accidents	S sabotage	Sh sharknado	SFl swine flu			
SF server failure	SS snowstorms	SoF software failure	T terrorism	TD theft of data	Th thunderstorms	To tornadoes
TS transportation strike	V vandalism	Vi viruses	WD water damage	Z zombies		

Lessons from Past Disasters

2012's Hurricane Sandy once again brought home the importance of comprehensive disaster recovery planning. With a cost of over $68 billion, Sandy caused organizations to face the question of whether they are truly prepared to recover quickly and continue operating after a disaster. Here are nine important takeaways.

1. Consider an off-site, real-time mirrored failover location on a separate power grid, so that you can continue operations in the event of a power outage or natural disaster localized to your immediate area.
2. Assign back-up roles in case key players are unavailable or missing.
3. Plan for all possible communication issues, including use of satellite phones, hotlines and Web alerts.
4. Establish accessible spending accounts for employees, make standing lodging arrangements near your recovery site and account for other logistics, like mail delivery and payroll.
5. Plan for extended recoveries, in case business is displaced longer than expected.
6. Keep your organization's documentation, scripts and business continuity planning handbook up to date.
7. Provide an alternative method of accessing your data and documents.
8. Be sure all vendor contracts are complete and up to date, including those with providers of media storage, insurance and fuel.
9. Plan for business continuity, because no one else will do it for you.

Disaster Recovery vs. Business Continuity Planning

The terms “disaster recovery planning” and “business continuity planning” are often used interchangeably, but they are two different concepts that work together as complementary components of an organization’s overall recovery and continuity planning.

Disaster recovery planning (DRP) is chiefly concerned with the recovery of systems and infrastructure components. By definition, it is limited in scope to a set of defined IT systems and infrastructure, with the ultimate goal of complete recovery within a defined timeframe and with a minimum of data loss. Because of the heavy emphasis on IT infrastructure, it may exclude non-IT business units such as accounting, marketing and sales, except in terms of software applications used by these departments. One issue with disaster recovery planning is that, because of the IT focus, incorrect assumptions may be made or subtleties or dependencies that are not hardware or application dependent—such as content management, document retention and security—may be missed.

Business continuity planning (BCP) is an attempt to blend the IT emphasis of disaster recovery planning with a larger-scope determination of which business components and functions must be prevented from interruption or, if interrupted, recovered immediately. It is an iterative process designed to identify these mission-critical functions and enact the policies, processes, plans and procedures that ensure their continuation if an unexpected event were to occur.

The exact functions covered by BCP vary by industry and may include processes that are not necessarily software applications, but also:

Infrastructure (office space).

Supplies (marketing materials and forms).

Human resources.

Basically, your organization can have a working disaster recovery plan without a working business continuity plan, but not vice versa.

Implementing a Business Continuity Plan

An effective business continuity plan is more than just the result of effective backups and data replication. An effective plan must not only be based on sound knowledge of your organization's culture and structure, but also on well-defined policies and procedures that make the plan a part of your daily operations, rather than something that is referred to only in case of emergency.

Your business continuity plan should include policies regarding:

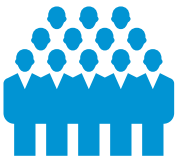
Emergency response procedures, such as reporting and tracking.

A public relations plan, determining who will speak with the media.

Damage assessment and insurance claims processing information.

A plan to handle phone calls, website updates, email and physical mail delivery. What if your building is destroyed and there is no office to deliver mail to? How will you update your website if your network is disabled?

An executive communication plan, with information on communicating with organizational management and other stakeholders, if applicable, as well as what your organizational response will be if key leaders are incapacitated or unavailable.



A communication plan for clients and vendors, because you don't want to lose contact with either group, especially if operations are disabled for a period of time.

An employee communication plan. How will you communicate with your staff if mobile phone, landline and other communications networks are destroyed? How will you locate employees to share crucial information with them? Also, your organization should have a plan in place to manage critical personnel data, such as emergency contact information, user IDs and network passwords, in case systems are down or destroyed.

Banking, especially regarding payroll and emergency cash access. This is an area that is particularly essential and challenging during a crisis, but is probably most overlooked when planning for a disaster. If you can't access funds during a crisis, your operations will grind to a halt, and disaster relief funding may not be instantly available.

Human resources systems that may not be immediately mission-critical, but will become important in the weeks or months until operations are back to normal. Consider back-ups of salary information, payroll information and personnel and tax information as well.

Implementing Your Plan

Have you considered ...

1. Workload division?
2. Hardware alignment/ positioning?
3. Storage strategy?
4. Data replication strategy?
5. Recovery and availability strategy?
6. Network connectivity and capacity measures?
7. Shared services and infrastructure components for base operating capabilities?
8. Virtualization alternatives?
9. Systems management mechanisms, command/control mechanisms, testing capabilities, physical and logical security features?

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

While most organizations are quick to consider their IT infrastructure when planning for a disaster, it is easy to forget paper archives. Paper is a familiar, yet extremely vulnerable, archival medium, particularly threatened by fire, flood and theft, and may be just as important as your electronic data, especially when it comes to pre-computer historical archives.

While most, if not all, electronic records are backed up in some format, paper records are often forgotten—and once they are gone, they are gone forever. The solution is enterprise content management (ECM) technology. With ECM software, a digital image of paper records is captured and preserved in unalterable format, guaranteeing its integrity.

Easily searchable and much more space- and cost-efficient than paper archives, digital archives should become a key factor in your organization's data storage and recovery planning. For example:

Monica Baccardax, IT Project Manager for the Faculty of Medicine at Dalhousie University Medical School, explains that her team was relieved "when they realized that our ECM system serves as a backup should paper documents be destroyed."

Law firm Arenson & Maas was particularly pleased to have an ECM "backup" in place when severe flooding prevented staff from working in the law firm's offices for more than four weeks. Authorized employees used the firm's ECM system to access records remotely, which was vital to producing billable work "with little disruption to business," says legal assistant Laurie L. Chappell.

Pulte Mortgage, meanwhile, notes that ECM plays a critical part in ensuring continuity of operations during the harsh Colorado winters. "In the past, if we heard a snowstorm was coming, we'd move all the paper loan files that were due to close to a hotel and house our processors there until the storm had passed," says CIO Gary Ives. "Giving them access to the information they need from home saves money and energy."

John Phillips, IT Systems Analyst at the Central Contra Costa Sanitary District, says, "We hope we never face an emergency that will demonstrate the benefits of having ECM, but we have to be prepared."

Without access to your data, key steps of your business continuity plan cannot be carried out and there is little hope of recovery.

Worksheet: Creating Your Business Continuity Plan

Creating Your BCP and Internal Audit Teams

In order to test business continuity planning (BCP) and disaster recovery (DR) compliance, a team of qualified, knowledgeable internal auditors should be created, reporting to a different member of the board than the BCP team reports to. This team of internal auditors must test policies and procedures to ensure that the BCP plan and process meet the compliance requirements.

Who will be on your business continuity planning team?

Who will they report to?

Who will serve as your internal audit team?

Who will they report to?

Risk Assessment

What risks are most likely to affect your organization, given your industry and physical location?

When considering risks, think beyond the accepted natural disasters, and don't forget to consider things like civil unrest, sudden changes in demand or hardware failure.

Are key systems backed up regularly enough (and are they able to be restored quickly enough) to ensure that availability of data meets specific business, legislation and standards requirements?

☐ Yes ☐ No

Are key systems' availability ensured using uninterruptible power supplies (UPS), failover/hot-standby facilities or other contingency measures?

☐ Yes ☐ No

Is the organization able to operate effectively without key personnel?

☐ Yes ☐ No

Is it clear who is the "second in command" in each department?

☐ Yes ☐ No

Are there at least two staff members who know how to carry out each key job?

☐ Yes ☐ No

Is the organization able to operate effectively without key systems (not just IT systems — telecommunications systems, manual systems, etc.)?

☐ Yes ☐ No

Are contingency manual processes in place in case key systems fail?

Is the organization able to operate effectively without key locations?

☐ Yes ☐ No

Are contingency locations available in which business can temporarily be carried out if a site/location is unavailable?

Are all important prevention mechanisms in place to avoid or reduce the effects of system failures or damage caused by floods, fires, terrorist attacks and so forth?

Take into account firewalls, intrusion prevention/detection mechanisms, auditing/logging, sprinkler systems, closed-circuit TV cameras, security staff, physical security mechanisms (such as passcodes, keycards, receptionists, keys and locks, security fences and building design).

☐ Yes ☐ No

The risk assessment area of business continuity planning can be tested by internal auditors by obtaining a copy of the risk assessment/business impact assessment documentation, and ensuring that it covers all the required systems, locations and personnel.

Conducting a Gap Analysis

A gap analysis of needs and capabilities will help you determine, in a high-level way, how able your organization is to meet the basic requirements of business continuity. This review process is the responsibility of the BCP team.

Have you had a security assessment carried out by an independent assessor (CISSP certified auditor or independent security consultancy)?

☐ Yes ☐ No

Have you conducted scenario testing of your BCP, such as a simulation of a terrorist bomb attack on your organization's headquarters, or simulation of a virus attack bringing down the network?

☐ Yes ☐ No

Changes to be made:

Have you checked to ensure that a backup plan for each key system has been implemented correctly?

☐ Yes ☐ No

Changes to be made:

Can backup personnel produce the backup tapes for these key systems when requested?

☐ Yes ☐ No

Changes to be made:

Are data restoration requirements met?

☐ Yes ☐ No

Changes to be made:

Are firewalls, intrusion detection/prevention systems, authentication systems (login, passwords, etc.) and logging/auditing systems operating effectively?

☐ Yes ☐ No

Changes to be made:

Are logs being reviewed and acted upon on a regular basis?

☐ Yes ☐ No

Changes to be made:

Are appropriate physical security measures in place and functioning effectively?

For example, security personnel are patrolling key areas regularly, visitors are always accompanied, security fences are in place, closed-circuit TV cameras are in place and are being watched, and security passes are required to access key areas of buildings.

☐ Yes ☐ No

Changes to be made:

_____

_____

_____

Are there procedures and policies in place to prevent data integrity or availability being compromised?

For example, checks and controls ensure data integrity, and separation of duties ensures that no single person can seriously affect data integrity and/or availability.

☐ Yes ☐ No

Changes to be made:

_____

_____

_____

As part of this gap analysis and review process, your BCP team should conduct regular reviews to identify any changes that should be made as a result of:

- Changes to legislation.
- Changes to the way business is carried out. (For example, a merger that adds a new business location to the plan or discontinues a business relationship with a partner, removing a location from the plan.)
- New experiences or information. (For example, many organizations have reviewed their BCP and DR plans in the light of 9/11, Hurricane Katrina, etc.)

How often will your BCP team review the plan?

_____

Who will be responsible for determining when the BCP should be reviewed?

_____

This review process can be tested by internal auditors in the following ways:

- Obtaining copies of the reports of any external auditors, consultants or security assessors.
- Obtaining copies of any minutes/agendas of meetings involving the BCP plan and process.
- Reviewing documentation of testing scenarios, such as test plans and test results.
- Requesting proof that any issues/problems identified were acted upon and resolved. Proof can include logs, change request documentation, printouts of software or hardware configurations, etc.
- Specifying dates for which the backup team should provide the backup tapes of all the key systems, and verifying that the backup tapes are restored effectively and correctly within data-restoration timeframes.

Developing Your Business Continuity Plans, Policies and Procedures

Data recovery procedures

List your strategies to handle:

1 Workload division

2 Hardware alignment/positioning

3 Data storage

4 Data replication

5 Recovery and availability

6 Network connectivity and capacity measures

7 Shared services and infrastructure components for base operating capabilities

8 Virtualization alternatives

9 Systems management mechanisms

10 Command/control mechanisms

11 Testing capabilities

12 Physical and logical security features

13 Reporting

14 Tracking

Call Lists/Communication

It should be clear who should be called in different scenarios, and their contact details should be widely available to all who need them.

Executive Communication Plan

Who will communicate with management and other stakeholders?

What will your organizational response be if key leaders are incapacitated or unavailable?

Employee Communication Plan

How will you communicate with your staff if mobile phone, landline and other communications networks are destroyed?

How will you locate employees to share crucial information with them?

How will you manage critical personnel data, such as emergency contact information, user IDs and network passwords, if systems are down or destroyed?

Client and Vendor Communication Plan

How will you communicate with your clients?

How will you communicate with your vendors?

The internal audit team can test this requirement by requesting a copy of the latest call list and calling the people on the list to ensure that the telephone numbers are up to date and that the people listed know what to do in various scenarios. It's useful to keep a copy of the call list, and a log of the results of calling the numbers, for use by the external auditors, who will later use this evidence to ensure compliance.

Public relations plan

Who will speak with the media?

Damage assessment and insurance claims processing information

Who will be in charge of contacting insurance agents?

Where will the information be stored? How will it be accessed?

Other Procedures

Banking Emergency Procedures

How will you handle payroll?

What if you need emergency access to cash?

Human Resources Systems

These systems may not be immediately mission-critical, but will become important in the weeks or months until operations are back to normal.

How will you back up salary information, payroll information and personnel/ tax information?

Phone, Web and Mail

What if your building is destroyed and there is no office to deliver mail to?

How will you update your website if your network is disabled?

How will you handle incoming phone calls?

Ongoing Auditing

Business continuity should be an ongoing process, concerned with the development of strategies, policies and plans that will provide protection of existing modes of operating within the organization, or will provide alternative means of carrying out that organization's business in the event of disruption that might otherwise result in loss to the organization.

This aspect can be tested by the internal auditors by asking the BCP team for the following:

- Proof of regular meetings: minutes, agendas, notes, presentation slides, etc.
- Regular scenario test runs, such as test plans and test results.
- Evidence of recent change management (such as logs showing ongoing changes) and reviews to the BCP plan (for example, version history of the BCP plan and associated documents).

How frequently will your audit team test your business continuity procedures?

Information derived from "Corporate Governance, Business Continuity Planning and Disaster Recovery" by Michelle Sollicito, retrieved from http://www.informit.com/articles/article.aspx?p=427373&seqNum=3.

Notes

Ready to see Laserfiche in action?

Schedule a free 30-minute demo with a Laserfiche document management specialist

Thanks for reading our Ultimate Guide to Business Continuity Planning. We hope it helped answer some of your most pressing questions and point you in the right direction.

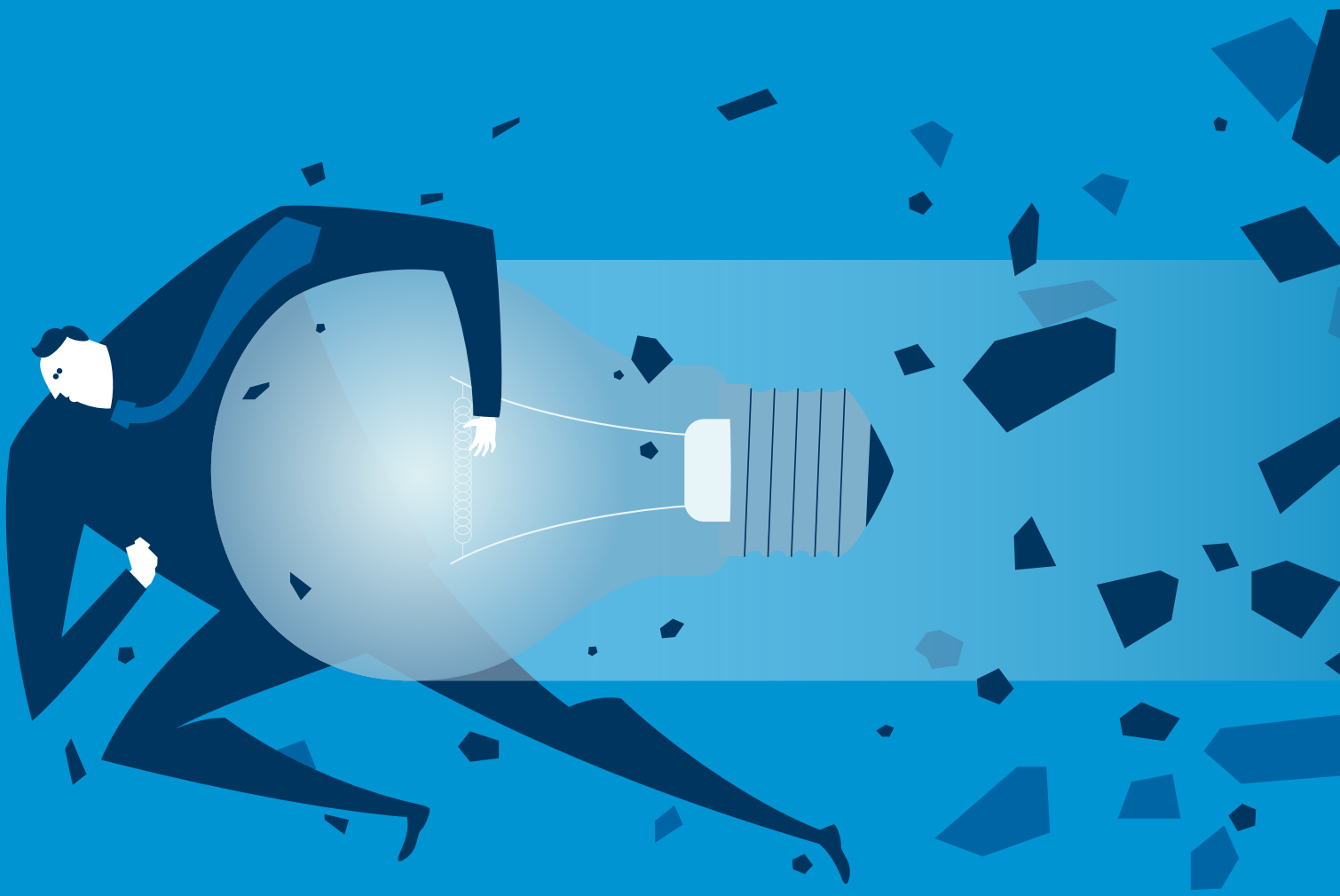
Still, there's nothing quite like speaking to an expert and seeing a solution in action firsthand. That's why we're happy to offer you a free 30-minute demo.

This 30-minute demo will get right to the heart of your document management challenges and demonstrate the many Laserfiche features that will enable you to cost effectively meet your organizational goals.

Click here to schedule your demo

www.laserfiche.com/demo

This demo is, of course, free of charge and without obligation.



THE ULTIMATE GUIDE TO

BUSINESS CONTINUITY PLANNING

About Laserfiche

Since 1987, Laserfiche® has used its Run Smarter® philosophy to create simple and elegant enterprise content management solutions. More than 34,000 organizations worldwide—including federal, state and local government agencies and Fortune 1000 companies—use Laserfiche software to streamline documents, records and business process management.

EVERYTHING YOU NEED TO KNOW TO BUILD
THE CASE FOR BUSINESS CONTINUITY PLANNING

Laserfiche®
Run Smarter®

www.laserfiche.com