Acronis

WHITEPAPER

Business continuity: Shifting from passive planning to active risk mitigation and ensuring resilience

Small and medium businesses (SMBs) are just as likely to be a target for cybercriminals as enterprises. It is no longer a question of if, but rather when a business will be targeted. Businesses can prepare for multiple contingencies by considering other disruption events through this lens. Disruptions may directly affect an organization or third party service providers down the line.

Ransomware attack on Kaseya

Kaseya is a managed services provider (MSP) with office locations around the world that provides a unified IT management and security solution directly to IT departments as well as other MSPs. Kaseya automates IT management for SMBs around the world.

In 2021, Kaseya systems were targeted by ransomware. Attackers gained access through a zero-day vulnerability in the company's VSA web interface, which allowed them to circumvent login security controls. Attackers deployed ransomware through a fake update within the system's automated software update tool.

A reported 800 to 1,500 businesses, including 50 direct customers, were affected either through service interruptions or by the ransomware itself. However, since Kaseya provides a solution for IT MSPs, reports estimate thousands of businesses who were not direct Kaseya customers were also impacted.

Organizations most affected by this ransomware attack were SMBs, including:

- Dental clinics.
- Accountants.
- Supermarkets (800 stores in Sweden were forced to close due to malfunctioning cash registers).
- Schools and kindergartens.

Ransomware targets small organizations

In another incident, an estimated 240,000 QNAP network attached storage (NAS) devices were encrypted with ransomware. Attackers used brute-force credential attacks and exploited known QNAP vulnerabilities to enter networks. Small businesses and home offices were specifically targeted in these attacks.

Cybersecurity researchers believe this series of attacks on small organizations were intended as "practice rounds" for attacks on larger enterprises.

SMBs' reliance on technology has increased over time. These businesses face many of the same challenges as large enterprises in planning for risk and managing security.

What is business continuity planning?

Business continuity planning (BCP) is a practice that guarantees continued business activities during a major disruption. In business continuity planning, the first step is identifying assets, followed by formulating a clear plan to protect them.

A business continuity plan is more than just an extensive informational document — it also includes specific instructions, policies and procedures for maintaining systems and operations. Business continuity will look different for each business, but the planning process itself will be similar.

There are some common elements in all business continuity plans.

Identifying key business areas

It is important to get a clear picture of what you intend to protect. The first step in business continuity planning is to identify areas that are central to your operations. These will include core business processes or functions.

Prioritizing critical elements

Critical and time-sensitive processes and functions should be addressed first. These will include core business functions and revenue-generating activities, as well as identity and access management.

Identifying interdependencies

Interdependencies between business areas and functions can complicate restoration and recovery efforts. Identify these ahead of time to understand how they work together.

Determining acceptable downtime

Depending on the nature of a crisis, downtime for some functions may be more costly than for others. Functions that meet financial and legal obligations will be ranked as having a shorter acceptable downtime.

Acceptable downtime is the longest time your business can tolerate a downed function before it causes irreversible damage to the organization and its reputation. Downtime is never a welcome scenario, but one that must be anticipated ahead of time.

Determining what to recover

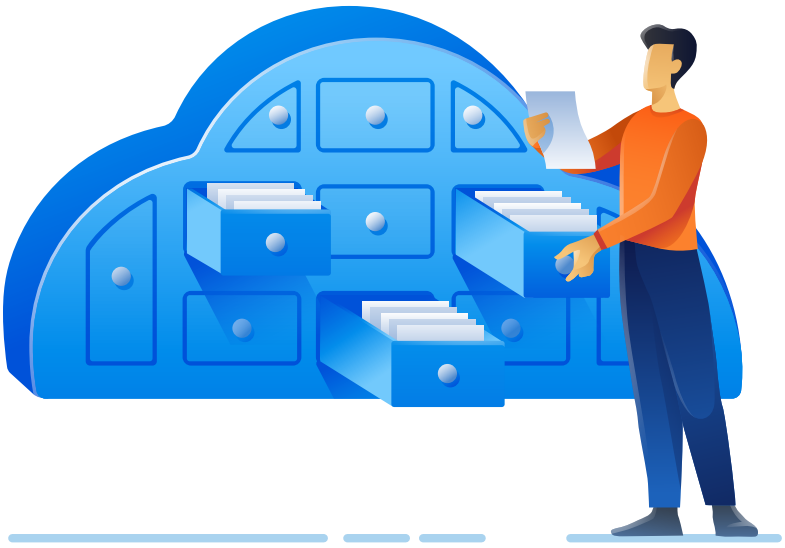
Once you have determined acceptable downtime, carefully consider what to recover and how quickly. Consider seasonal business cycles, days of the week, and time of the day, as well as how a disruption would affect operations, customers and employees. The importance of each function determines its recovery priority:

- Determine the shortest time a function can be down before long-term damages occur.
- Low priority functions can quickly become high priority if they are not addressed.
- Identify and review achievable recovery strategies for each function.
- Can functions be outsourced or handled at an alternate location? How long can this tactic be maintained?
- Can employees work from another location (e.g., remotely) if their primary work location is affected?

Work closely with key staff and stakeholders to identify the functions, systems and data most critical for recovery efforts.

Documenting the plan

A continuity plan requires careful documentation. A plan without documentation relies on the institutional knowledge of staff employed at the time. Documentation ensures the plan remains usable, even after personnel changes.



What is risk assessment?

Risk assessment is the process of identifying and evaluating potential risks for all aspects of an organization's operations. The process surfaces potential weaknesses before disaster strikes. Risk assessment helps you prepare for worst-case scenarios and achieve operational stability so your business can survive.

Conducting a risk assessment

Organizations of all sizes should assess operational risks. SMBs may not realize that they face many of the same risks as enterprises. The Verizon 2023 Data Breach Investigations Report revealed that small businesses suffered 41% more breaches than large enterprises, with 68% more of them resulting in a confirmed data disclosure.

Assessing the impact and likelihood of threats

Risk assessment begins with estimating the impact and likelihood of potential hazards or threats on assets. Hazards may include natural disasters, cybersecurity, pandemics and fires. Assets include people, business operations, property, equipment and financial or contractual obligations. Risk assessments focus on how hazards and threats might impact assets.

Risk analysis: Applying risks to assets and sites

The risk analysis process requires a detailed analysis of potential adverse events, consequences, and their likelihood of occurring. It digs into detailed scenarios and control factors to gauge potential effectiveness against risks that might affect business assets and locations.

Mitigation

Risk mitigation planning is an iterative process. How an organization handles risk mitigation will depend on customer needs and the severity of the risk itself. Risk mitigation planning is the process of outlining mitigation options to reduce threats.

Risk mitigation approaches include:

- Assuming or accepting the risk: Acknowledge and accept the risk without taking action to control it.
- Avoidance: Choose actions that eliminate or reduce risk to avoid the risk.
- Control: Control risks to minimize the impact or likelihood of the event.
- Transfer: Transfer accountability, responsibility and authority to other stakeholders or a willing third party.
- Monitoring: Monitor risk factors for changes affecting the nature or impact of the risk.

As part of your risk mitigation strategy, you should:

- Understand users and their needs during an unplanned, adverse event.
- Seek out experts and take advantage of their expertise.
- Accept that there are recurring risks.
- Recognize that not all risks require mitigation.

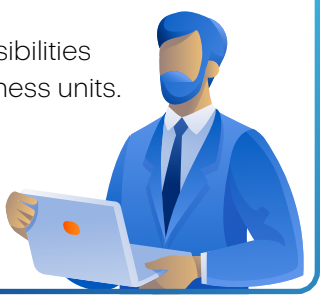
Cost evaluation

Evaluate the cost of mitigation versus the cost of impact. Know what to expect before a major disruption event ever occurs. Identify appropriate mitigation methods and determine the costs and benefits for applying them.

Developing a plan

Develop an action plan using information gathered during the risk assessment stage. Establish a clear outline with the following steps:

- Identify key stakeholders.
- Develop a communications strategy for internal and external audiences (employees, customers, public).
- Assign teams responsible for specific aspects of the plan during execution.
- Identify systems backup and restore locations and functionality.
- Assign actions and responsibilities across departments / business units.



How legacy planning and assessment fall short of today's requirements

Legacy continuity and risk assessment planning methods do not quite meet modern business needs, as they fail to account for an ever-changing threat landscape. This could lead to inaccurate recovery strategy scenarios, because they do not include managing multiple disruptions at once. For example, the COVID-19 pandemic revealed how parallel crises can swiftly topple response plans. Shifts in markets and workflows combined with an ongoing worldwide pandemic have completely disrupted the way we do business.

Duration of events and issues

Planning may cover multiple disruption event scenarios with a focus on limited or localized interruptions with a short duration. The planning process builds from a specific framework instead of focusing on varied outcomes. Planning is siloed and may focus on a specific line of business without considering the rest of the organization. The way individual assets function together is routinely ignored.

Multiple vendors disrupted

Multiple vendors can be affected, creating disruptions in a chain reaction. Third-party vendors can face a multitude of issues, which may affect customers further down the line:

- Inadequate tracking and management of risk.
- Lack of transparency into interdependencies between third parties.
- Narrowly focused disaster recovery and business continuity planning.
- Lack of strategic vision when outsourcing critical skills and functions.

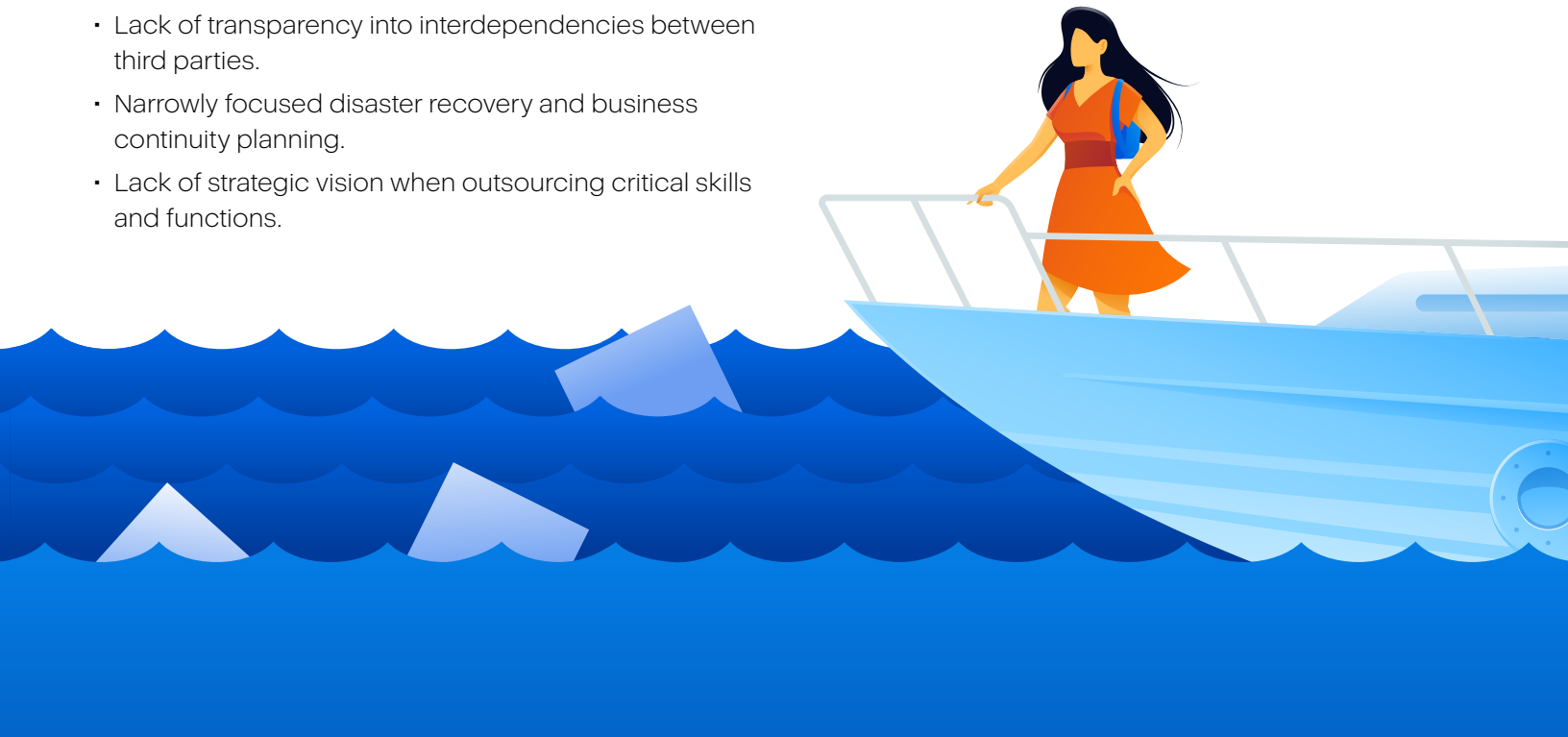
Traditional risk assessment does not consider extended operations disruptions. Since many modern business operations are interconnected, SMBs can share a space with large enterprises. An event that seems to happen far away can affect multiple vendors in different ways, triggering a disruption in SMB operations.

Lack of employee training

Traditional risk assessment does not consider the true impact of insider threats. Cyberthreats are constantly evolving, and there remains a need for continued training — yet many organizations fail to offer cybersecurity training to address current or rising threats.

Employees — including those who have some understanding of cyber risks — may not practice safe computing.

Employees are unaware of today's increasingly more sophisticated cyberthreats and do not know how to identify them. In many organizations, there is a wide gap between knowledge and risk awareness. Employees who complete cybersecurity training once or twice a year are unlikely to identify potential cyber risks. Even basic cybersecurity training is lacking. Cyberthreats are on the rise, and SMBs may not have a formal training program in place or the budget to support one.



Too many single points of failure

A single point of failure is a person, piece of equipment, application, or other resource without redundancy. Single points of failure can include network devices or servers, highly specialized equipment, and employees with specialized knowledge who alone complete the required work for a particular function.

An organization with multiple single points of failure is more vulnerable to the impact of an unplanned outage or attack. Staffing risks include a lack of knowledge transfer when an employee leaves or goes on extended leave — no other employees can complete the job. Specialized equipment failures can lead to extended disruptions. Aging network or server equipment may result in data loss, in addition to worsening security issues — especially if they are in service beyond the equipment's service and support lifecycle.

A 2020 KPMG advisory highlighted many weaknesses in legacy business continuity planning methods during a multi-event convergence that included a pandemic, changes in work location and equipment, as well as major market shifts. The findings included compelling data from massive shifts happening all at once, which were not considered in existing business continuity plans.

Tools to prevent, detect, respond to, and recover from modern cyberthreats

Thinking critically about all aspects of prevention, detection, response and recovery is essential for preparation. Modern threats to systems operations look a little different. More than one disaster can and will happen at once.

Compound hazards are the new reality, as exemplified by the confluence in recent years of a global pandemic, economic turmoil, supply chain issues, natural disasters exacerbated by climate change, and steadily increasing cyberthreats that use artificial intelligence as a force multiplier. Vendors can now offer better analysis to prepare for and address multiple disasters at once.

Remote work leads to a new reality

Remote work has forced organizations to reconsider network security and all the new devices connecting to internal resources. Ongoing remote work arrangements require a novel approach to security — not all devices are company owned and managed; personal devices bring added security risks. Employees connect from home and are responsible for home network maintenance and security. Security becomes an even greater concern when employees can connect to internal resources from networks they do not control.

Better scenario evaluation leads to less ad hoc planning

A proactive approach to scenario evaluation means less ad hoc planning by working to predict potential interruption events before they happen (as much as is possible). Consider typical hazards and risks along with cyber events and data breaches, and their potential to damage brand reputation.

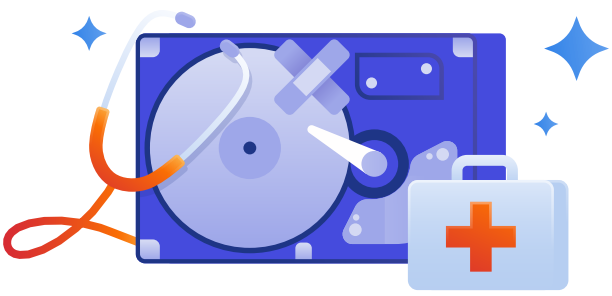
When businesses are proactive, they can focus more on recovery strategies.

Fewer manual steps to navigate unforeseen hazards

Comprehensive enterprise risk management can be combined with artificial intelligence and automation, resulting in fewer manual steps — thereby allowing faster response and recovery. However, no longer relying on employees to handle specific complex tasks can be a challenge, depending on the nature of the outage or disaster.

Better preparation and easier training

Fewer resources are required for recovery tasks. Employees need less training to use tools and are no longer managing multiple recovery tasks manually.



Proactively review plans and outcomes

Developing a plan, only to file it away, significantly reduces its effectiveness to address new or different challenges in the future. Proactively review plans and outcomes instead — review your business continuity plans regularly. After a significant disruption, you can evaluate how well the plan worked in execution.

A continuity plan review is an active process that includes a number of steps.

Testing and preparedness

Testing your plan against potential adverse effects is essential. An untested plan is as helpful as having no plan in the first place. A regular testing cycle will surface gaps in your plan. A thoroughly tested plan gives you flexibility to respond to ever-changing threats.

Examining the effectiveness of policies and procedures

Examine policies and procedures for fitness against your current needs. Question the effectiveness given your present circumstances, equipment, and personnel. Consider the following questions:

- Do your procedures continue to fulfill their original objectives?
- What can be adjusted to address changes since the last review (or the first edition) of the plan?
- If you have already experienced a major threat, did the policies and procedures give the appropriate personnel adequate access and control during the event?
- Were communications timely and regular?

Software updates and security patch management

Having a plan for system updates and patch management is helpful, but both must be applied (and tested) regularly. The Cybersecurity and Infrastructure Security Agency (CISA) maintains a list of routinely exploited software vulnerabilities that can be remedied by applying software patches. CISA recommends installing updates and applying security patches as soon as is reasonable for your organization. MSPs offer automated solutions that manage software updates and patches to ensure they are applied on a timely basis.

Enforce a zero trust policy

Zero trust is a security model which guides deployment and operation for systems engineered according to so-called zero trust principles. The zero trust model is used to secure sensitive information, systems and services. Zero trust assumes a breach is inevitable and may even be in progress. This approach to security allows users to access only the information they need at a given time (the principle of least privilege or PoLP). All user connections are verified before they are allowed to continue. Enforcing a zero trust policy is only possible on systems designed to work within this security model.

Staff training

IT staff training is an important aspect of disaster recovery and business continuity planning. Staff must understand their roles and responsibilities as they relate to the continuity plan. Unit supervisors can provide support and training, and generate awareness about the plan to their direct reports. Employees unfamiliar with the plan will have great difficulty executing it in a situation where time is limited.

Conclusion

Service disruptions will happen, disaster will strike, and cybercriminals are sure to target even the smallest businesses. Simplify cyber protection for your business by deploying an efficient, all-in-one cloud solution instead of managing multiple tools for endpoint protection, anti-malware, antivirus and data backup.

Safeguard your data from any threat with Acronis Cyber Protect — the only cyber protection solution that natively integrates data protection and cybersecurity.

Be prepared for any disruption, wherever it begins. Acronis Cyber Protection Operation Centers (CPOC) form a global network for threat protection and monitoring. Acronis CPOC sends real-time alerts on malware, vulnerabilities, natural disasters and other global events that may affect data protection.