Pushing On Through the Face of Adversity

How to plan for risk-assessed, scenario-based business continuity planning.

Traditional approaches to Disaster Recovery and Business Continuity have focused on major single-point failures, involving "fail over" to hot backup sites and cloud-virtualized services. A disaster event handled using these legacy models eventually required a "fail back" to the pre-disaster configuration – an error-prone and problematic process in its own right. Often fail-back failed, leaving databases with inconsistent structures and lost transactions.

The whole fail-over/fail-back process was documented in a step-by-step book that you could practice repeatedly and test periodically. In theory, if everything worked your DR/BC test had no impact on day-to-day operations. That worked about a third of the time, according to a 2016 survey from the Data Recovery Preparedness Counsel. In fact, fully 25% of respondents reported never having tested their DR/BC plan1.

Today's businesses are much more fragmented than they were in 2016, and disasters are much more nebulous. Nowhere is this more evident than in service sectors like finance, healthcare, and transportation. On March 29, 2021, for example, the UK's Financial Conduct Authority (FCA) published final rules that create a new operational framework for banks and fintech operators.

In the US, the Federal Reserve (Fed), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) published a similar paper itemizing sound practices to strengthen operational resilience. The need for resilience is even greater given the interconnected nature of financial and medical services, where outages at one firm or third party service provider can propagate to their partners in the same sector.

Can DOT, EMEA-APAC, and HIPAA be far behind?

These service sectors need to focus on three key changes to DR/BC planning. First, business IT assets don't reside all in one place, making fail-over/fail-back a much less viable solution. Second, most businesses already are using cloud virtualization, raising the question of how to handle cloud service outages. Third, modern disasters are not quite so clearly demarcated: they can start gradually, and grow in intensity, requiring on-the-fly adjustments to business continuity plans.

[1] Mellman, Roger (2016). Why you should think more about disaster recovery. Kansas City Business Journal, July 28, 2016 https://www.bizjournals.com/kansascity/news/2016/07/28/why-you-should-think-more-about-disaster-recovery.html

SAI360
RISK FROM EVERY ANGLE

The new approach to DR/BC is aimed at letting a business push on through in the face of changing rules and resource availability. A sudden staffing shortage might be one scenario. Supply chain disruption might be another. A data breach could be a third. Called scenario based planning, this strategy begins with risk management processes to identify which disaster types have highest priority, based on their likelihood and financial impact.

This white paper introduces the concept of risk-assessed, scenario-based business continuity planning. It describes risk assessment methodology and CapEx and OpEx costs involved, strategies for monitoring key metrics to detect an imminent disaster, and the ways to ensure continuous security protection throughout a business disruption. You'll then be well positioned to begin your own journey.

Risk Assessment

Business continuity resilience has three attributes that differentiate if from traditional DR/BC:

- Before an incident begins, your system is designed to accommodate expected risks and to continue operating, possibly at an acceptably degraded level, in the face of unexpected risks;
- When an incident starts, your system uses these built-in capabilities to maintain mission-critical services despite adversity, resisting total disruption as long as possible, with the ability to continue operating in degraded mode indefinitely.
- After an incident ends: system implementers learn from, and make changes to accommodate, unanticipated conditions.

Traditional DR/BC plans don't accommodate these differences. Engineers often write them, and engineers aim to solve problems. Not surprisingly, engineers tend to jump right into the nuts and bolts of keeping operations running, relying on data backups, spare hardware, and DR/BC planning documents.

Today's businesses can't start their DR/BC planning with this approach, because there are simply too many variables. Which services are most important? Which are most likely to fail? Which failures are the most expensive? What are alternative means to continue operation? These are questions that can only be answered by conducting a formal risk assessment (RA). Without RA, you'll waste time and resources on less important business continuity measures – and almost certainly miss the most important ones.

You use RA to identify and prioritize potential vulnerabilities facing your business. It's essential prerequisite to BC planning. RA implicitly incorporates a business impact analysis (BIA), to predict business consequences when particular functions or processes get interrupted. The subject matter experts (SMEs) in your key lines of business should develop your BIA, not the IT department. For each business unit, a BIA should detail:

- The immediate and long-term economic damage resulting from an outage.
- The labor and cost to recover from an outage.
- Existing mitigations in place to prevent disruptions.
- The minimum level of service necessary for continued operation in the face of an outage.

With a BIA in hand, you're ready to being the actual RA processes:

Itemize critical assets

You must identify your most valuable assets in order to protect them. Assets include databases, applications, websites, and computing and storage resources. The staff using these resources are also assets that need protection.

It's important that you not think of assets as implementation items, such as a server with a particular serial number, or a database at a specific cloud provider. You're listing conceptual assets here, because in the BC planning process you may well substitute a different underlying implementation of a particular asset.

Identify risks and prioritize them by probability and severity

It's a truism that the most probable risks are the least severe. For example, a common user error in a database may trigger a brief outage in a non-critical system, but restoring the file from a local backup readily repairs it. On the other hand, a natural disaster such as a flood, while far less likely, is far more damaging.

Assigning numeric values to risk probability and severity, and then multiplying them to generate a risk score, is one way to rank risks to mitigate first in your BC planning. A good way to enumerate risk is through disaster scenarios. These scenarios are of foreseeable events, such as flood, fire, and social disruption. Identify must-have critical resources necessary to continue day-to-day

operations, even with degraded performance. It's better to operate at half speed than at no speed at all.

Look for hidden dependencies.

For each identified risk, search for weaknesses that can cause processes to fail, such as 2FA depending on a single cloud provider. These hidden dependencies are by definition not obvious, and this is one part of the RA process that might require input from your IT staff. They understand behind-the-scenes workings of your systems and are thus more likely to call out hidden dependencies.

Document financial losses and recovery effort for each risk from your BIA.

The BIA you prepared earlier for each business unit will let you document the cost to business and recovery labor for any given risk. Later, when building your BC plan, you'll aim to employ transparent fail-over mechanisms to continue operation with little to no downtime.

The end result of your RA will be a detailed document itemizing every risk, its impact on revenue, its potential for affecting multiple systems, and how much capital and operational expense you'll incur to mitigate the risk.

Proactive Monitoring

It's been common for businesses to have reactive, rather than proactive, stances where business continuity is concerned. "When disaster strikes, break out the disaster plan," is the rallying cry. But in today's highly dynamic environment, that may be too late to avoid serious business losses.

It's much better to keep an eye on your businesses critical metrics, called key performance indicators (KPIs), for an early warning when something is amiss in your enterprise. For example, inventory levels falling below a certain threshold may presage supply chain problems caused by a cyber attack at a business partner. Another common metric ripe for KPI monitoring is customer sales levels, because customers are often like coal mine canaries in predicting business issues.

You should establish baselines for your KPIs and then monitor then continuously, using IT automation tools to present them on a business intelligence (BI) dashboard. This gives decision makers a birds-eye view of business health, which could provide essential lead time when reacting to a disaster or major market change.

You can assign each KPI signal a specific level of importance, depending on the amount and direction of its deviation from the norm. Sometimes a KPI varies wildly, which is often symptomatic of a business process that is overreacting to some stimulus. For example, an inventory shortage may trigger a large parts order, which may in turn result in unnecessary products being manufactured, causing backorders in products that have customer demand. In such cases, it's often best to freeze all changes until the chaos subsides.

Only your business unit SMEs) can identify and develop response plans for KPIs. Your SMEs can intuit what is going on in their businesses processes, and advise you on the measures to take to get back to normal. In particular, SMEs will recognize an impending business failure and advise you on when to invoke BC measures to bypass the problem.

For instance, if a cloud provider outage inhibits or delays customer order processing, the BC plan may be to switch to a different cloud provider immediately. In general, your systems should be able to treat cloud providers as interchangeable. If they can't, you need to solve that problem before moving forward. Typically a particular cloud provider is chosen based on cost or performance, but during an outage, those factors become moot. It's better to have an expensive provider that is working than a cheap one that is not.

Maintain Security

In the heat of battle during a disaster, it's easy to cut IT security some slack in the name of expediency. "Let's get everything working first, and then go backfill the security holes," is a common thought process. But this ignores the fact that businesses are most vulnerable to attack during an emergency, something hackers readily exploit. Human error is the most frequent cause of a security incident during disaster operations. Either a user failed to follow policy, given the unfamiliar procedures triggered by BC plans, or IT failed to anticipate a security loophole caused by BC processes. A data breach results, which on top of the disaster could well be fatal to the enterprise.

Security vulnerabilities are a risk, just like any other, and should be managed right at the start of the RA process. You must identify single points of failure in your authentication, encryption, and firewall measure, and make sure that backup components implement the same security policies. One way to do this is with a central security orchestration system, which contains a single repository of all security policies. When a business process or data flow switches to a recovery path, the orchestration tool will have replicated those polices in the new environment, whether that be a premises server or a cloud-based one.

FINAL THOUGHTS

Security events often cross premise/cloud boundaries, making intrusions difficult to detect. Hybrid cloud security is the process of ensuring the security of data both at rest and in transit, as well as monitoring across cloud providers and on-premises components. It uses advanced instrumentation, in the form of Security Information and Event Management (SIEM), to both detect and quantify security intrusion events. If detected quickly enough, an intrusion can be isolated so that most IT infrastructure continues to operate normally.

For example, SIEM can detect a ransomware encryption event – one of the most damaging cyber attacks – long before a ransom notice appears, letting IT isolate the affected system. Hybrid security also typically provides "single-pane-of-glass" visibility into security monitoring components, greatly reducing security human costs.

Overcoming Adversity

Now that you understand the importance of risk assessment, how to identify CapEx and OpEx costs of BC, KPI monitoring for early warning, and maintaining security during a business disruption, you're ready to get your business into BC boot camp. Instead of failing over, you'll prepare to push on through.

Interested in learning more about SAI360's business continuity solutions?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination