Masters of disaster recovery

How highly resilient organizations excel
Cloud, mobile, social, the Internet of Things—technologies like these are reshaping business, making us more productive, flexible, connected and responsive. But our growing reliance on their 24/7 availability also puts us more at risk when disaster strikes.

Why are some companies better at mastering disaster recovery in the face of today’s “always-on” expectations? The difference comes down to an integrated strategy that leverages advanced technologies and a robust testing program.
In enterprise IT today, everything is more connected. Everything needs to be available all the time. Everything is becoming data-driven. Your employees, consumers and partners expect that the information, products and services they need will be “always on” —available when, where and how they want them.

To meet these demands, systems are increasingly integrated, distributed and interdependent—which can create lots of potential vulnerabilities. Linking more critical systems together to meet higher expectations complicates disaster recovery and security. When one link in the chain breaks or comes under attack, the impact can ripple throughout the business.

Nearly 40% of organizations have had to execute their disaster recovery plan due to a service disruption in just the past two years.

In our study of 310 business continuity (BC) and disaster recovery (DR) professionals, nearly 60 percent of organizations have executed their disaster recovery plan due to a service disruption. And about 40 percent of companies have had to do so in just the past two years. Compounding the problem: recovery times aren’t improving, and the business impact of downtime is increasing.1

Disruptions happen. Anticipating problems is critical. But even with the best preventative measures in place, you need to have a battle-tested recovery plan.

The problem: There has never been more a challenging time to master disaster recovery.

Social Signals

More than 99,000 social media discussions about disaster recovery and business continuity occurred in our six-month listening period.2

About the study

To gain insight into today’s most effective business resiliency strategies, the IBM Center for Applied Insights surveyed 310 disaster recovery and business continuity professionals in the United States and Canada. The respondent base consisted of BCDR leaders primarily in executive and managerial roles, including more than 60 percent who are Directors of IT or CIOs. Survey participants work for companies spanning 19 industries, and ranging in size from less than 100 employees to more than 10,000.

About the IBM Center for Applied Insights

ibm.com/ibmcai | ibmcai.com

The IBM Center for Applied Insights introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.
Disaster recovery and business continuity professionals work in a more demanding and complex business environment than ever before. About 55 percent of study participants say the top challenge they face is incorporating an increasing number of business-critical systems into their recovery plans. For example, more businesses consider mobile applications to be essential tools. This means these apps need a level of protection equal to what’s provided for more traditional critical systems, such as logistics, call centers or email workloads.

As the number of critical apps and workloads grows, so does the degree of IT integration. The result: more potential points of failure that DR teams must manage. The increasing number of connection points with suppliers and business partners only serves to compound the issue.

Nearly half of DR leaders name security breaches and cybercrime—which are increasing in scope and sophistication—as another top challenge to their organizations’ resiliency. And it’s clear many organizations are losing ground, with half of business resiliency leaders admitting their organizations aren’t prepared to handle service disruptions from cyberattacks.

Still, a group of companies stand out among the rest, showing a greater mastery of disaster recovery. What makes them different?
Disaster recovery’s treacherous terrain

Business resiliency professionals face a host of steep obstacles to meeting always-on expectations.

- 55% Including an increasing number of critical systems in DR plan
- 49% Addressing cybersecurity risks
- 48% Managing more points of disruption due to greater IT integration
- 38% Demonstrating strong ROI for DR investments
- 37% Meeting tighter RTOs and RPOs*
- 33% Finding IT professionals with DR expertise
- 30% Meeting rapidly rising business leaders’ expectations of DR capabilities
- 30% Using analytics to better predict service disruptions
- 45% Securing funding needed to meet DR objectives

*Recovery time objectives (RTOs) and recovery point objectives (RPOs)
An elite group drives to the top

Despite the significant challenges, a group of highly resilient organizations leads peers with disaster recovery strategies that encompass integrated plans and robust testing. Less than a third of BCDR professionals are part of this elite segment of disaster recovery Masters. By comparison, some 44 percent rate as Specialists, while 26 percent come in as Tacticians.

**Masters** adopt an enterprise-wide strategy for disaster recovery with more frequent and rigorous testing.

**Specialists** have begun to improve their testing and security, but still haven’t quite made the leap to an integrated approach.

**Tacticians** are still testing systems individually and somewhat infrequently, while treating disaster recovery as primarily an IT issue.

Our findings left little room for doubt: Masters’ results rise above the rest. They report significantly better performance against key disaster recovery metrics. For example, Masters are 1.5 times more likely than Tacticians to report that they’re ensuring the rapid resumption of revenue generating business processes—which is key to maintaining customer relationships—when disruptions happen.

Masters are also 2.5 times more likely to report meeting recovery time goals and controlling recovery costs, achievements that demonstrate the value the DR team contributes to their organization’s success.

Overall, Masters are four times more likely than Tacticians to report their disaster recovery capabilities are better than others in their industry.
Who’s leading the climb to higher resiliency?

Facing challenges head-on, a group of highly resilient organizations ascends above the rest with integrated BCDR plans and frequent, robust testing.

- **Masters**
  - Frequent and robust testers, holistic planners
  - 4x more Masters say they’re outperforming industry peers on DR
  - 2.5x more likely than Tacticians to report they’re achieving recovery time objectives
  - 2.5x more likely than Tacticians to report they’re lowering recovery costs

- **SPECIALISTS**
  - Fairly well-rounded testers, but siloed planners

- **TACTICIANS**
  - Occasional testers, IT-focused planners
  - Siloed, fixed approach and occasional, primarily compliance-driven testing
Reaching the heights of business resiliency

Masters anticipate and plan. They forge a strong culture of collaboration between IT and business, taking into account new technologies, business priorities and risks when planning for disaster recovery.

They test and assess. Practice, practice, practice. That’s how Masters improve their response times and extend the scope of their business resiliency programs.

Masters also respond and recover faster. They exploit the right technologies so that they get critical business processes back up and running quickly.

Textron takes disaster recovery to the next level

Textron, a multi-industry company known for such brands as Bell Helicopter and Cessna, understands the high stakes at play in business resiliency.

Disaster recovery approaches at some enterprises don’t always include critical infrastructure and security services or consider broader dependencies in deciding which assets to get back online first. Textron takes a more holistic approach to resiliency planning, beginning with a roadmap of critical assets and obscure dependencies. “Previously you would ask ‘what applications are necessary to keep your business running?’” says Textron CIO Diane Schwarz. “You evaluated ERP, manufacturing and inventory systems, but may not have considered some of the broader systems required to support the operations. Enterprises need to take into account the critical assets in a network, not just the financially significant ones,” she says.

Textron also recognizes the importance of having the flexibility to adjust resiliency strategies as business needs change. The company turns to technology and trusted partnerships to help it move between cloud, shared floor space and hybrid solutions.

Practice makes perfect. The company tests its recovery plans three times annually. Putting its enterprise-wide disaster plan to the test often prepares the company for the smaller incidents that it, like others, face daily.

Textron believes it’s not enough to put everything in a facility out of town and know that it will be there when you need it. “One aspect that is often overlooked is the talent perspective,” says Schwarz. “You need resiliency not just in your tactical architecture; you need it in your teams.”

Testing at Textron includes people from business units, application support, infrastructure support, project managers and power users along with support teams from service providers.
Scale disaster recovery like a master

Masters surpass their peers in four major areas of disaster recovery.

- Approach DR strategically
- Integrate security
- Leverage new technologies
- Test rigorously
Masters approach disaster recovery strategically

These leaders are more than twice as likely as Tacticians to maintain an integrated disaster recovery plan. Masters involve senior management throughout the organization in resiliency planning. With such high stakes in play, the board is watching. Masters know this and actively include the board in prioritizing investments based on the most critical business needs.

Management’s involvement comes with clear marching orders. Seventy-one percent of all respondents say business leaders expect information security risks to be factored into disaster recovery plans. And half of responding DR professionals explain that their DR investments come with a strong ROI mandate. Masters also include trusted external partners in their disaster recovery assessments more often—both ecosystem partners and DR planning experts.

Social Signals

There were 9,000 social media discussions on disaster recovery strategies and end-to-end planning in our six-month listening period.

<table>
<thead>
<tr>
<th>Tacticians</th>
<th>Specialists</th>
<th>Masters</th>
<th>Masters vs. Tacticians</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involve board in DR planning</td>
<td>34%</td>
<td>47%</td>
<td>73%</td>
</tr>
<tr>
<td>Maintain an integrated DR plan</td>
<td>19%</td>
<td>26%</td>
<td>46%</td>
</tr>
<tr>
<td>Involve external experts in DR planning, execution &amp; evaluation</td>
<td>21%</td>
<td>34%</td>
<td>44%</td>
</tr>
<tr>
<td>Integrate suppliers into overall testing</td>
<td>9%</td>
<td>12%</td>
<td>39%</td>
</tr>
</tbody>
</table>
Masters collaborate with risk and security experts

An enterprise-wide view of potential vulnerabilities can make disaster recovery plans more targeted and effective. Masters incorporate enterprise security and risk management as a critical part of disaster recovery and business continuity planning. They’re 3.5 times more likely than Tacticians to involve their company’s CISO in disaster recovery planning and five times more likely to involve the CRO. They also include security policies in their disaster recovery testing, simultaneously vetting both their recovery plan and their security practices.

### Social Signals

8,000 disaster recovery social discussions related to security topics.

<table>
<thead>
<tr>
<th></th>
<th>Tacticians</th>
<th>Specialists</th>
<th>Masters</th>
<th>Masters vs. Tacticians</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involves CISO in DR planning</td>
<td>16%</td>
<td>36%</td>
<td>57%</td>
<td>3.5x</td>
</tr>
<tr>
<td>Integrates enterprise security and risk management into DR</td>
<td>21%</td>
<td>32%</td>
<td>52%</td>
<td>2.5x</td>
</tr>
<tr>
<td>Have security policies in place and working during DR tests</td>
<td>4%</td>
<td>16%</td>
<td>47%</td>
<td>12.0x</td>
</tr>
<tr>
<td>Involves CRO in DR planning</td>
<td>6%</td>
<td>19%</td>
<td>30%</td>
<td>5.0x</td>
</tr>
</tbody>
</table>
Masters leverage new technologies

These pacesetters often tap innovations such as cloud, analytics and mobile to restore crucial business processes rapidly. They’re more likely to provide real-time mobile updates during a disruption and use the cloud for recovery.

With downtime destroying revenue, Masters are also more likely to deploy virtual networks, replication and storage to improve resiliency and get operations back up and running faster.

Finally, Masters don’t wait to react. They’re about 15 times more likely than Tacticians to uncover risks and vulnerabilities using diagnostic analytics. Plus they’re more likely to use predictive analytics to spot potential disruptions. These tools are deployed not just for recovery but to diagnose the root cause of looming issues, anticipate risk and prevent outages.

SOCIAL SIGNALS

One in every five social discussions about disaster recovery revolves around technology.

And 67% of those technology discussions focus on cloud.

* Cannot be calculated because denominator is 0—no Tacticians reported using predictive analytics.
Masters test rigorously

This elite group fine-tunes their recovery plans by testing them more frequently and thoroughly. For example, they’re 2.5 times more likely than Tacticians to test their disaster recovery plans at least annually and in many cases test as frequently as monthly or weekly. And they’re adaptive, updating future plans based on what they learn during testing.

Masters are vigilant, including testing requirements in service-level agreements. They’re also deliberate, maintaining consistency between their disaster recovery tests and their production environments.

**SOCIAL SIGNALS**

More than **2,500** social media conversations focused on disaster recovery testing during our listening period.

<table>
<thead>
<tr>
<th></th>
<th>Tacticians</th>
<th>Specialists</th>
<th>Masters</th>
<th>Masters vs. Tacticians</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test at least annually</td>
<td>34%</td>
<td>68%</td>
<td>89%</td>
<td>2.5x</td>
</tr>
<tr>
<td>Include testing</td>
<td>33%</td>
<td>43%</td>
<td>64%</td>
<td>2.0x</td>
</tr>
<tr>
<td>requirements in SLAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain consistency</td>
<td>13%</td>
<td>19%</td>
<td>55%</td>
<td>4.0x</td>
</tr>
<tr>
<td>between DR test and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>production environments</td>
<td>21%</td>
<td>34%</td>
<td>45%</td>
<td>2.0x</td>
</tr>
<tr>
<td>Adapt future plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>based on testing results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How can your organization master disaster recovery?

**Establish a strategic, integrated disaster recovery approach**

- Work together with internal leaders, including the board of directors, as well as with supply chain partners and knowledgeable industry experts.
- Base your strategy on a thorough understanding of compliance requirements.
- Consider the needs of both your business and its customers.

**Design a robust testing program**

- Test annually at a minimum, and develop the ability to test in real-time with ad hoc queries from any device.
- Continuously improve testing by incorporating insights learned from previous tests into DR plans.
- Extend testing across internal infrastructure, new mobile and cloud-based applications, and connections with supply chain partners.
- Benchmark yourself against DR industry leaders to pinpoint areas for improvement.

**Collaborate with security and risk leaders**

- Partner with risk teams to enhance DR compliance and governance.
- Engage your security team to integrate cybersecurity into DR planning.
- Consider having internal audit teams sign off on DR plans to further ensure you’re meeting regulatory requirements.

**Incorporate new technologies into DR plans**

- Explore using cloud, advanced analytics and mobile to respond more effectively and to prevent future service disruptions.
- Use social technologies to not only communicate system status and adverse events in real time but also to monitor economic, environmental or other external events that could disrupt business.
About the authors

Mike Errity is Vice President, IBM Resiliency Services North America for IBM Global Technology Services. His consulting, sales and delivery team works collaboratively with clients across all industries to assess, design and implement solutions to mitigate technical and operational risk. Mike has two decades of professional experience in business resiliency, seeing the evolution of client needs shift to be “always on” in the United States and globally, as he previously led this business line in the United Kingdom. Mike can be reached at merrity@us.ibm.com and via Twitter at @MikeErrity.

Rasheq Rahman is the North America lead for the IBM Center for Applied Insights, providing data-driven insights around resiliency, security and client transformation. Before joining IBM, he was involved in the commercialization of energy technologies and spent nearly a decade developing trading operations for several global investment banks. Rasheq can be reached at rsrahman@us.ibm.com and on Twitter @rasheqrahman. He also posts on the Center's blog.

Kelly McKenna is a Senior Analyst for the IBM Center for Applied Insights, providing thought leadership to provoke informed conversations among leaders in the digital age. In her current role, she conducts data-driven research on emerging business technology trends for forward thinkers and industry pioneers. Prior to joining the Center, she was an advisor for the IBM Global Technology Services division. Kelly can be reached at mckennak@us.ibm.com and on Twitter @k_mck120. She also posts on the Center's blog.

Contributors
Angie Casey
Laura DeLallo
Anurag Goyal
Tyler Kettle
Lindsey Reichelt
Notes and sources


2 The statistics provided in Social Signals are based on social listening for disaster recovery and business continuity terms across English-language blogs, forums, and tweets worldwide from June through November 2015. For more Social Signals on a variety of business topics, check out the IBM Center for Applied Insights blog series.