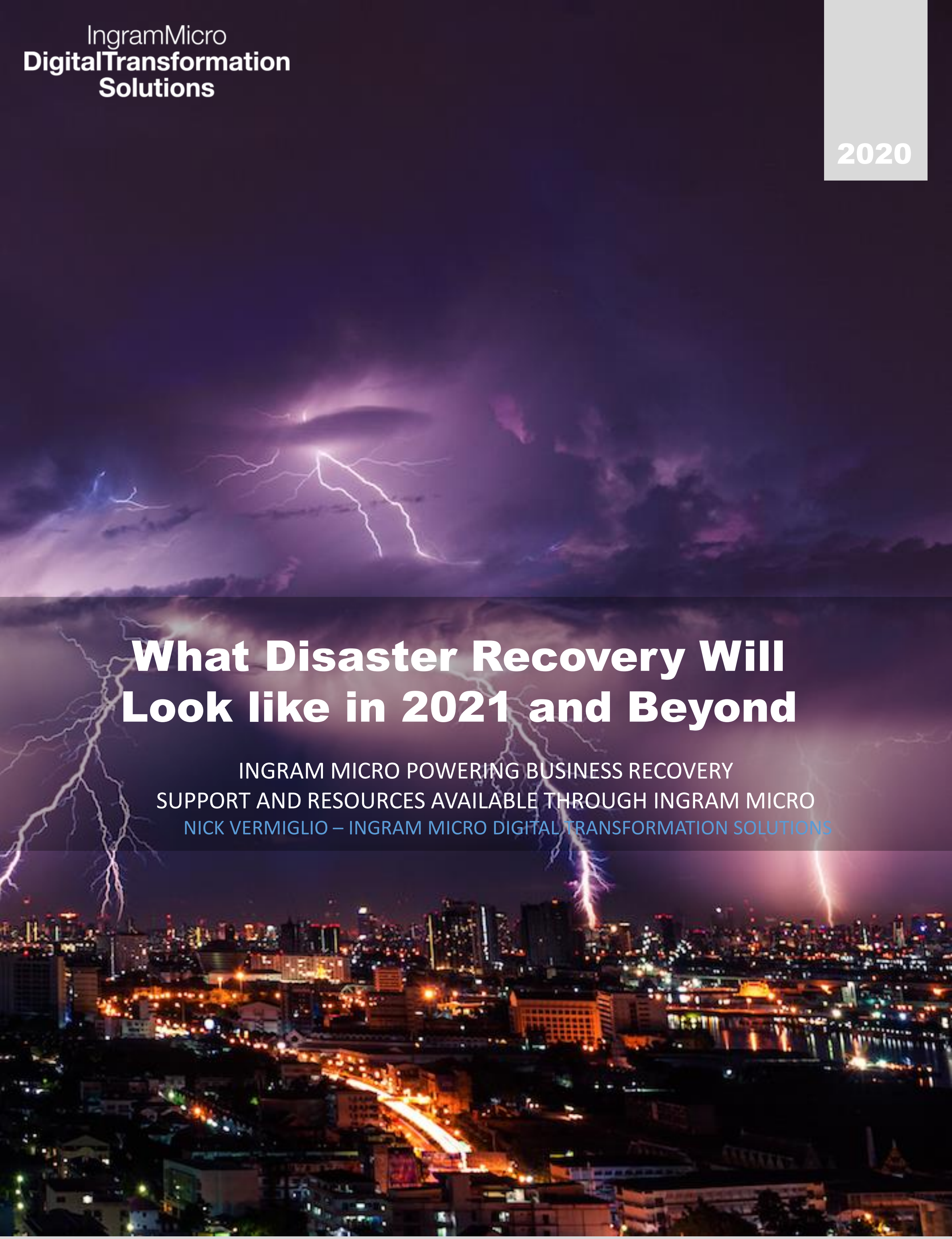
IngramMicro
DigitalTransformation
Solutions

2020



What Disaster Recovery Will Look like in 2021 and Beyond

INGRAM MICRO POWERING BUSINESS RECOVERY
SUPPORT AND RESOURCES AVAILABLE THROUGH INGRAM MICRO

NICK VERMIGLIO – INGRAM MICRO DIGITAL TRANSFORMATION SOLUTIONS

IN TODAY’S VOLATILE GLOBAL ENVIRONMENT, it’s more important than ever for organizations to develop a business continuity plan (BCP).

From political and economic uncertainty to the increased prevalence of extreme weather and health events, BCPs help businesses remain financially and operationally viable regardless of external circumstances or unforeseen events.

To reduce loss and mitigate risk associated with potentially crippling situations, business continuity strategies are relevant for all types and sizes of businesses, including insurance agencies.

In 2012, Hurricane Sandy left a trail of destruction from Maine to the Carolinas. In New Jersey alone, nearly 19,000 businesses sustained damages of $250,000 or more with total business losses estimated at $8.3 billion.

This report explains why businesses should make continuity planning a core priority and how technology plays a critical role.

It outlines best practices for minimizing the impact of unexpected events on business operations and financials: leveraging cloud-based solutions and data centers, using multiple types of digital communications and maximizing mobility.

Many of these innovative technologies may already be integrated into an organization’s operations. However, when used as part of a BCP, they can increase the return on investment of an organization’s existing technologies, while also protecting its most valuable assets: its reputation, customer loyalty and continuity of operations. Safeguarding these assets ultimately translates into maintaining, and even possibly bolstering, an agency’s revenue stream.

Organizations of all sizes, in virtually every industry and every region around the world, are investing heavily in technology to drive growth and increase competitiveness.

In this first annual Flexera 2020 State of Tech Spend Survey, they found that, overall, respondents are spending 8.2 percent of revenue on IT. Where is the money going?

The top three initiatives cited by survey participants are digital transformation, cybersecurity and cloud first/ cloud migration. These large-scale projects require substantial technology investments, so it’s not surprising that more than half of respondents say they expect to increase IT spend over the next year.

As companies make these large tech investments, however, are they getting maximum return? It’s likely that many are not. Survey respondents estimate that 12 percent of their technology spend is wasted. But research by Flexera and other industry experts puts the amount of waste at 30 percent or higher. For a company with a $250 million IT budget, that can be as much as $75 million down the drain.

Disaster Recovery and Business Continuance is a form of security planning that allows a business to maintain or recover infrastructure and systems following a disaster, and ultimately allows them to save the potential losses they could face. With good planning, a business should be able to resume normal operations by regaining access to hardware, applications, and data.

This is achieved with a disaster recovery /business continuance plan — a set of policies and procedures to follow in the event of a disaster.

The disaster that impacts a business may be anything from a natural event such as a flood or earthquake to one that is man-made, whether by human error, a device failure, or a cyberattack. The disaster recovery process involves a lot of planning and testing for a variety of possible circumstances, allowing businesses to reduce overall downtime and save time, money, and customer trust.

First, a risk assessment and business impact analysis needs to be carried out. Security vulnerabilities must be identified in order to draft an effective disaster recovery plan. Even when a disaster recovery plan is created, it must be tested and revisited on a regular basis.

Naturally, plans differ based on the type of disaster they're addressing, each offering varying immediate, intermediate, and long-term responses with specific responsibilities assigned to select staff members.

Aside from offering corrective measures in the event of a disaster, a disaster recovery plan should also have preventive measures in place as well as detective measures that help discover events that may otherwise be missed. It is important to remember that every business is unique. A data-loss event for one business can be exorbitantly more expensive than for a similarly sized business right across the street. It all depends on how that data is used (and how it's protected).

Calculating the average cost of data loss can be challenging, because it can vary widely depending on the size of the business and how valuable the data is. However, there is no disagreement that a typical data-loss event can be tremendously expensive.

Here are some telling figures:
In 2018 the global average cost of data loss was a staggering $3.6 million, or approximately $141 per data record. However, that research mostly focused on the costs of data breaches, such as theft of personal user data, login information and credit card numbers.

A leading Disaster Recovery/Business Continuance provider estimated that data loss costs U.S. businesses an average of $7,900 per minute during a datacenter outage.

A recent report by Verizon found that “small” instances of data loss (around 100 lost or compromised records) cost businesses an average of $18,120 to $35,730.

The same study found that large-scale data loss (100+ million records) costs an average of $5 million to $15.6 million.

On average, downtime from data-loss events costs small companies more than $8,500 per hour, according to 2016 figures from Aberdeen Group.

Depending on the company's size, Datto estimates that the costs of downtime can vary from $10,000 per hour to more than $5 million per hour.

Downtime caused specifically by ransomware has been surging over the past year. Datto found that the costs of these incidents has nearly tripled, from $48,800 in 2018 to $141,000 in 2019.

This emphasizes the importance of having an effective disaster recovery plan that allows a business to continue operations as normal. 93% of small businesses store data or backups in the cloud.

According to promising results from a Unitrends' 2019 survey, 84 percent of all businesses store data or backups in the cloud, with a further eight percent planning to do so within the next year.

Many organizations had become complacent and procrastinated about cloud adoption before the crisis and will now be acutely aware of their IT limitations.

This equals opportunity

"*We've seen two years' worth of digital transformation in two months*" Satya Nadella - Microsoft

Small enterprises have a higher adoption rate of cloud technology, with 93 percent of companies using it. This is compared to 82 percent of mid-sized businesses and 81 percent of large businesses. Using cloud backup offers several advantages including ease of access and affordability.

The report also found that cloud-based Disaster Recovery-as-a-Software (DRaaS) will be used by 59 percent of businesses by 2021. Currently, 36 percent of businesses use this, and a further 23 percent plan to add the technology within the next year.

A large portion of companies (55 percent) experienced five or more outages during that period. The same report reveals that IT decision makers believe that 51 percent of outages and 53 percent of brownouts are avoidable.

Of course, outages and brownouts have related costs, including lost revenue, compliance failure, and lost productivity. LogicMontor found that companies experiencing frequent outages or brownouts had 16 times higher costs than organizations that experience fewer such instances.
Source: LogicMonitor

About the Author:

Nick Vermiglio, *Sr. Technology Consultant*

Nick has over 40 years experience in Healthcare, Retail, Education, Manufacturing, Legal and Financial vertical markets. As well as providing consultative support with respect to end user development/operations procedures in major verticals.

Nick's current focus at Ingram Micro is Backup & Recovery/Disaster Recovery/ Business Continuance and he is the Subject Matter Expert providing consulting support during 9/11 as well as other major initiatives for firms conducting business in major verticals. He is also focusing on developing assessment solutions and services that support the Digital Transformation efforts of Ingram Micro, our partners and their customers at all levels.

Please contact Nick for any other additional questions you might have about these solutions!

For More Information on this topic please contact the DXS Team at dxsolutions@ingrammicro.com

And for more resources visit: playbooks.ingrammicro.com

*The information complied here has been provided by various sources that are credited in this paper