STEPS FOR BETTER BUSINESS RESILIENCY

"Be Prepared" is the motto of the Boy Scouts of America, but it could be the motto for business resiliency as well. Here are a few basic tips to help you "be prepared."

Business resiliency is not disaster recovery. Business resiliency plans ensure uninterrupted processing for essential functions. Disaster recovery plans address the restoration of service after a catastrophic event. Most businesses need both, but business resiliency is something that comes into play almost every day.

FOCUS ON HOW YOUR BUSINESS MIGHT BE AFFECTED

Rather than trying to identify all the potential causes of a business interruption, think about how your business would be affected. Most business interruptions fall into one or more of these categories:

- Hardware
- Facilities
- Network/telecom
- Software
- People

HARDWARE FAILURE CONSIDERATIONS

If your computer hardware fails or is otherwise unavailable, you generally have two alternatives — move to a back-up system or invest in a high-availability computing environment where the failure of a component does not compromise overall performance.

The back-up system is less expensive but it can mean that you can't process for hours or even days in some cases. High availability generally avoids that kind of outage, but it comes at a cost. You will have to determine, based on your business needs, the level of investment required.

It doesn't really matter *why* the computer hardware is unavailable. You need to be prepared regardless of the reason.

EFFECT OF A FACILITIES OUTAGE

A facilities outage in many ways is like a hardware failure — you have to have an alternative. For some businesses, that means working from home via remote access, and that's a great plan provided those key resources can get into the system. Can your remote access system handle an exponential increase in simultaneous users?

Technology that works fine when a handful of people are remote might be inadequate if dozens or hundreds of people need access at the same time. And don't forget about phone coverage. Voice mail and call re-routing are important tools during a facility outage.

As you move through the rest of the five business resiliency considerations, you'll find that they become progressively more difficult to address, but there *are* ways to deal with each consideration, although how you will address them may vary based on the unique nature of your business.

PNC®

REASONABLY ANTICIPATED THREATS

Let's move to the third building block of business resiliency — reasonably anticipated threats. What concerns you the most? Where is your system most vulnerable? If you have a single incumbent in a critical job and that person is out for some reason, that's a problem.

If you have 50 people doing a similar function, any one person being out doesn't represent much of a threat to your ability to provide essential services. If you are on the Gulf Coast where severe weather can be a problem, a facility outage might be a bigger risk than it is in Pittsburgh where major storms are relatively infrequent.

Listing your reasonably anticipated threats will help you identify the situations you are most likely to encounter, and that should help you prioritize your investments in business resiliency.

FAILURE MODE EFFECT ANALYSIS

For those who want a more formal prioritization process, consider a Failure Mode Effect Analysis or FMEA. With the FMEA model, you assign values to the likelihood of an occurrence, the impact of a failure if it were to occur, and the cost or difficulty of recovery from that failure. By multiplying those values, you get an overall severity rating that can help add some objectivity to a process that might otherwise be highly subjective.

MANAGING COMPLEX EVENTS

As much as we all hope to avoid them, disasters do occur, and the best business resiliency plan in the world won't help you avoid the impact of something like Hurricane Katrina or the Sendai earthquake in Japan. In that case, you'll experience outages in two, three, four or possibly all five of the risk categories mentioned earlier. For example, a building fire might take out your facility, your computer hardware and your network connectivity all at the same time.

Clearly, that's a much more complex event to manage, but by assembling the pieces you've already compiled, I think you'll find a logical progression to follow in order to restore service.

Taking steps to ensure that your business continues to perform essential functions in the face of an emergency need not be an overwhelming task if the plan is developed step by step using a proven process.

FOR MORE INFORMATION

There are many sources of information on business resiliency for those who would like to learn more. Established sources for professional education include:

- The Association of Contingency Planners
- The Business and Industry Council for Emergency Planning and Preparedness
- The Business Resiliency Certification Consortium International
- Continuity Central
- The Department of Homeland Security
- The FEMA Emergency Management Institute

For more information, contact your Relationship Manager or visit pnc.com/treasury.

The article you read was prepared for general information purposes only and is not intended as legal, tax or accounting advice or as recommendations to engage in any specific transaction, including with respect to any securities of PNC, and do not purport to be comprehensive. Under no circumstances should any information contained in this article be used or considered as an offer or commitment, or a solicitation of an offer or commitment, to participate in any particular transaction or strategy. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own counsel, accountant or other advisor regarding your specific situation. Neither PNC Bank nor any other subsidiary of The PNC Financial Services Group, Inc. will be responsible for any consequences of reliance upon any opinion or statement contained here, or any omission. The opinions expressed in this article are not necessarily the opinions of PNC Bank or any of its affiliates, directors, officers or employees.

PNC is a registered mark of The PNC Financial Services Group, Inc. ("PNC").

©2014 The PNC Financial Services Group, Inc. All rights reserved.

CIB ENT PDF 0514-063-178620