Avoiding Downtime

The C-Level Guide to Managing Technology Risk

FirstLight

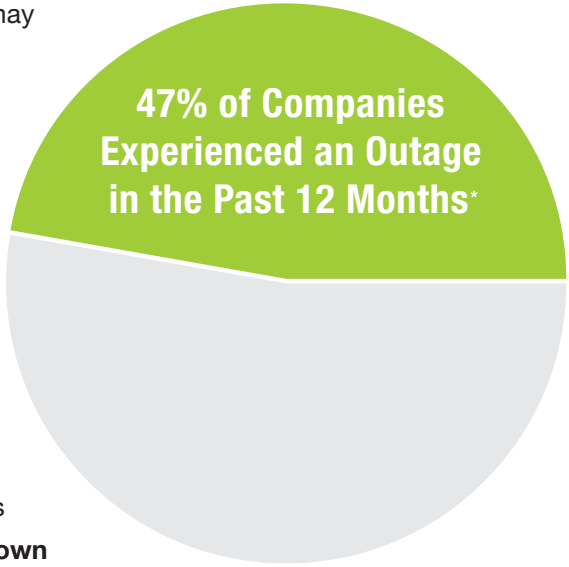
C-Level Executives are Part Historians, Part Strategic Thinkers

If you're an executive, your responsibilities likely span from finance and accounting to policy and strategy. You also may be in a position to play the role of company historian, evaluating past performance and highlighting the impact that it will have on your investors and stakeholders. But as an executive, your primary responsibility is managing risk. No one understands the importance of risk more than a great executive. You're the voice of reason in the room when the company wants to speed ahead introducing new products, new markets and new strategies. You use both the microscope and the wide-angle lens for all that goes on in your company. But how aware are you of risk as it relates to technology? How involved are you at managing the risk that a catastrophic technology failure could have on your firm?

What may seem like a promising short-term outlook could turn into a nightmare if you don't understand the importance of avoiding downtime. Play a strategic role in understanding the importance of your firm's technology and the associated risk if that technology fails to perform or is unavailable. Put simply, your job shouldn't involve explaining to your board why the numbers took a nose dive because of a preventable technology failure.

It's Not About Bits and Bytes, It's About Business Outcomes

All too often, IT managers spout off technical terms that executives don't fully understand in order to get funding approval. That strategy may work in some cases, but when it comes to IT resiliency, that can't be the case. As an executive, you need to know how protected your company is from potential technology disasters. Your employees rely on critical applications to get work done, and if they can't do that, then your customers' needs won't be met and you then have a domino effect. Without access to technology, your company immediately begins losing money in the form of missed opportunities, lost productivity and goodwill.



Ask yourself an honest question: if your firm lost access to critical technologies and applications would you know what happens next? **In a five-year span, 1 in 3 companies will declare a full-blown disaster.**** Do you have the confidence that your company can handle even a run-of-the-mill, everyday outage? If you lack this technical understanding, then you're not alone; you didn't go to school for computer science. But what you should know at least at a conceptual level is what your IT department has planned if such an event were to occur.

*Source: https://www.zerto.com/dr-to-the-cloud/disaster-recovery-service-draas-infographic/

**Source: "Disaster Recovery 101 eBook" by Zerto

Is Your Company Living In The Past?

For many years, disaster recovery solutions were too complex and too costly for most companies to implement. Only certain industries were able to spend money on the systems, the data centers and the labor that it took to build a truly resilient approach to IT. The C-level executives at the rest of the firms were forced to forgo the expensive route of a true disaster recovery (DR) solution. But that was then, and this is now. Technology today is too important for DR to be an afterthought.

Many IT decision makers may be living in the past when it comes to disaster recovery. As an executive, you need to know that DR is no longer complex or cost prohibitive. In fact, like all aspects of technology, DR has improved to the point where you no longer have the excuse not to have a solid DR solution in place.

Warning Signs That Your DR Approach Isn't Where It Should Be

The most obvious warning sign that your DR approach may be lacking is that your company may have experienced an outage that you struggled to recover from. Did you lose valuable data? Did you experience an embarrassing amount of downtime that had to be explained both internally and externally? While these experiences may seem common, they shouldn't be. Like a vaccine that prevents a disease, DR solutions exist today that can prevent significant downtime from ever occuring.

If you've been lucky enough to avoid an outage, then you want to make sure you aren't living on borrowed time. Consider asking your IT leader the following question: "If our Data Center failed, what would you do next to help us get back on our feet?" This may seem like a drastic scenario, but a stress test of your plan is the only way to know for sure if it will work. Here's a quick cheat sheet to make sure you understand the answer you might get:

"We have a geographically-redundant DR solution that replicates our applications and data in real time. My staff is instructed to click the button to begin the automated recovery and within minutes our systems are back online at the secondary site."

Congratulations! If you get this response from your IT team, then it would appear that you have the two major pieces of DR covered: a simplified, automated recovery and a negligible loss of data and time.

"We back up our data off-site every night. If something happens to our data center, we'll work to resolve the problem and then use that backup data to recover our applications and data. We have spare hardware at our branch office that we can use if needed."

This might work in some cases but even for the easy-to-handle outage, you'll have a loss of many hours of data and a manual process that carries an unknown length of time to recover.

"We back up the data every night."

It's not just about having the data backed up. It's about downtime and how long it will take to recover during an unexpected outage. Having your data sitting by itself without the ability to access it has no value to your company. You need your applications to come back online quickly.

Trust, But Verify

As a follow-up question, ask how often your IT department has truly tested and certified that their DR plan will work. If you have an overly complex plan, then it's very likely that your IT staff doesn't have the time or interest in truly testing it. They may be apprehensive about how well it will work and may fear that testing it could actually cause the very downtime you're trying to avoid. When it comes to IT resiliency, "trust, but verify" is always a good strategy.

Are You Part Of The Problem?

As an executive, you may be removed from the day-to-day activities of your IT department but your leadership has influenced them. How well have you supported their efforts to build IT resiliency? Have you helped them "think differently" about disaster recovery? Does your IT staff fear that DR won't be supported because it's a cost they know you'd rather avoid? Unless you're a CIO, you may not have day-to-day IT responsibility. But as a major officer of the company, you have the strategic imperative to make sure that your technology not only enables productivity, but that it won't become your downfall.

Want to learn more about FirstLight's cloud-based DR solution?

Visit FirstLight.net/DR

You can also e-mail us at sales@firstlight.net or call 800-461-4863 to begin a discussion about how to improve your IT resiliency.