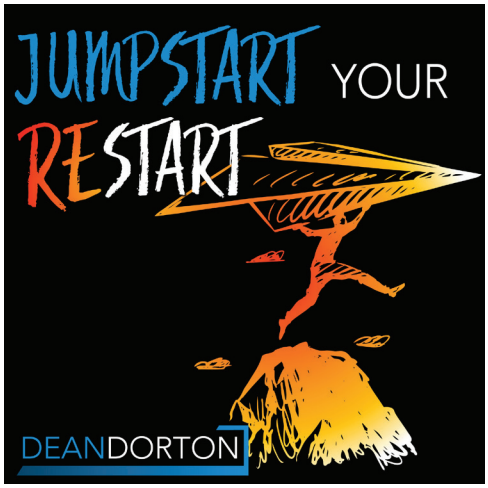

EPISODE 4:

Five Ways to Make Sure Your Business is Disaster-Ready

Podcast Transcription

Host: Jason Miller | Director of Business and Technology Consulting

Our goal for this podcast series is to provide different perspectives on many issues being faced by businesses and organizations during this difficult time and how to begin preparing your organization for returning to operation. I was tempted to say return to normal—but, we have all had to wrap our heads around the fact that we aren't going to return to normal. We're now working toward a New Normal.

Working toward a New Normal means change, and a lot of it. Humans struggle with change—often even resistant to change. I do a lot of my professional work in the area of technology. As we all know, technology changes at a rapid pace. I have seen studies that the rate of change in technology has actually surpassed human's ability to adapt to that change and the gap continues to grow each year. I believe this pandemic has forced us to accept change at an unprecedented pace.

In today's episode, we will discuss five things you can do to help make your organization disaster-ready. Very few organizations were prepared for this global economic shutdown. Some businesses or industries were able to pivot and appear to have been more prepared than others, but I would contend that very few organizations had actually considered this scenario and planned accordingly. Many were just fortunate to be in an industry that was less impacted or had some processes or contingencies in place for other reasons that helped them to minimize the impact.

A New Normal is not necessarily a bad thing. In Episode 2, David Bundy and Justin Hubbard discussed 10 ways to make your business better than it was before the pandemic, addressing changes that can help provide improvement. As we evaluate these changes, we need to consider the possibility of another short-term shift back to a shelter-in-place scenario. We also shouldn't forget to prepare our organization to be ready for the next unknown disaster. One additional thought I'll challenge you with: Don't consider this exercise as only taking into account negative events. Preparing your organization for a disaster can also help improve normal daily operations at the same time.

I've spent a great deal of my career in IT compliance. One major focus of IT compliance hinges around risk evaluation, risk mitigation, and planning for disasters and business continuity. In my business consulting role, I like to leverage that experience and expand these important concepts beyond IT. How can you improve your operations and prepare your entire organization for the next disaster? Let's face it: it's impossible to consider and plan contingencies for every possible disaster. Case in point, very few organizations considered or were prepared for a global health pandemic. Now, we get to add this scenario to our playbook. Let's discuss some key considerations to help prepare your organization for future disasters.

1. **Be intentional.** Don't leave this important task to chance. Do you have a formal team and set of processes to evaluate organizational risk? Does this team include the appropriate individuals or representatives from across the organizations? Does it, or should it, involve outside professionals who can often bring additional perspective? We often get caught up in the bubble of "our world" and lose sight of important outside factors that could impact us. Other organizations or industries may have important lessons learned that could be applied to your situation. What are the critical concerns and scenarios that could interrupt and impact your organization?

2. **Have a plan.** Once you understand your organizational risks, have a plan for contingencies or playbooks on how your team will respond. IT departments spend a great deal of time and resources on disaster-recovery. Let's face it: technology fails. We often say the question is not if it will fail, but when it fails. We implement backup solutions, we write detailed instructions on processes to follow when going to a backup, and we test them regularly. This scenario is very narrowly focused. It provides a plan for when a piece of hardware or software fails and sometimes a plan for what to do when a natural disaster occurs. Expand this process to your entire organization for a business continuity plan and consider as many of the risks as you can. Build plans for how your team will deal with these scenarios if they ever become your reality.

EPISODE 4: Five Ways to Make Sure Your Business is Disaster-Ready

Podcast Transcription

3. **Revisit regularly.** The risk assessment and development of a business continuity plan should be a continual exercise. We're in a constant mode of change, and every change inside and outside of your organization can have an impact to your risk and your plan. Case in point, we all have a new risk to plan for now. Our business continuity plans all need to be re-evaluated continually. Notice I chose the word "continually" rather than "regularly." I used to recommend that organizations perform a regular risk assessment or review of their business continuity plan. Regularly implies some interval of recurrence. Most organizations would say these two items are revisited annually. But it doesn't take a global pandemic to force the need to evaluate your risk or update your plan. Small changes within your organization or industry forces could create new risks and require you to change your business continuity plan at any time. These functions need to become naturally occurring events and not forced annual activities.

4. **Be nimble.** Consider ways to make your organization more nimble. As we saw with the COVID-19 situation, organizations had to adapt and change very quickly and frequently. As we were preparing our own changes at Dean Dorton, the changes would change before we could get them communicated. We would work out a plan to make the next required change and before we could communicate these changes to our team members, the government would issue a new set of guidance. This forced us to stop and think how our organization can be more nimble and react when we have to shift away from business as usual. Is your leadership team prepared to make quick decisions? Do you have tools in place to adequately communicate to your team, your customers, or other key constituents? Are you tied to or dependent on something physical that you may not be able to access, whether that be a brick and mortar location or a big piece of IT hardware? Are there new solutions out there that allow you to mobilize more effectively and efficiently? Here is one of the biggest questions: is your organizational culture one that embraces or resists change? An organization with a culture that resists change doesn't stand a chance at surviving in a world of constant and quick changes. We need to evaluate how well we prepare our teams for change. The more open to change we can make our organization, the more nimble we become.

5. **Consider layered protection.** There is not a single solution to account for every possible disaster. As we've seen, it is impossible to consider every scenario. There will always be something we haven't considered. I revert back to concepts we employ in technology. In cybersecurity, we preach a layered approach to cyber defense. If one layer of security fails, hopefully one of the other layers will hold and provide the needed protection. The final layer of protection that we recommend is cyber insurance. We know there is no absolute defense, so we have insurance protection to help minimize the financial burden and business impact if we experience an incident that we couldn't plan for and defend against. Throughout the COVID-19 pandemic, I heard many organizations ask if their general liability insurance would help them cover lost revenues. No one knew the answer. No one had considered this. Be sure you understand what insurance coverage you have in place and what it does and does not cover. Does it provide you with that final layer of business continuity protection? Make sure you're proactive in working with your insurance provider to understand how it can be your final layer of protection in your business continuity plan.

I hope I've challenged you to take this opportunity to think about how to prepare your organization for future disasters or crises. The most important takeaways are be intentional and work to make your organization as nimble as possible. Create a culture that embraces change rather than resists it. Change is not going away and organizations who embrace it will be more likely to survive the next global crisis.

Tune in text time to hear more about technology solutions for making your organization's future last. Good luck as you work to create your new normal and jumpstart your restart.