FROM DISRUPTION TO RECOVERY & GROWTH:

A TECHNOLOGY PLAYBOOK FOR BUSINESS LEADERS

PRESENTED BY

Managed IT, Security, & Cloud Services

INTRODUCTION

How resilient do you think your business was to the recent disruption?

When the COVID-19 work-from-home mandate hit, those with the right policies and infrastructure in place managed the massive shift with not too much disruption. Others experienced tremendous challenges.

But what started off looking like a temporary situation has turned into a longer-term proposition, from many perspectives. Even when employees do start returning to the workplace, it likely will be done in stages, and business may have to accomodate many new practices.

"EFFECTIVE ORGANIZATIONS CAN AND DO LEARN FROM CHALLENGING TIMES"

Few of us have experienced this level of disruption in our lifetimes. But with disruption comes lessons learned, and it forces us to take stock. Effective organizations can and do learn from challenging times.

Now is the ideal time to review your operations and turn this into a positive growth experience, not only speeding recovery but preparing for future success.

INTRODUCTION

Many of the business leaders we spoke to, including IT leaders of small and mid-sized companies, are looking to technology to help them transform into a more effective organization. The ability to use the cloud, mobile devices, new collaboration services and enhanced security practices can all help improve workforce efficiency and employee engagement, and business resiliency.

With that in mind, we've created a framework that focuses on five critical areas for you to explore:

1. **Business Continuity Planning**
2. **Technology Infrastructure**
3. **Communication & Collaboration**
4. **Cybersecurity & Risk Mitigation**
5. **Processes & Automation**

BUSINESS CONTINUITY PLANNING

The very first thing you need to do is document what went well and what did not during the recent disruption. Your goal here is to gather enough data to revise your Business Continuity Plan.

Didn't have one in the first place? Now would be a great time to get that done! Note that a true business continuity plan is very different from a disaster recovery solution.

Business continuity is a comprehensive written plan for maintaining business operations during a disruptive event. This is different than disaster recovery, which is focused on how you restore the interrupted services.

"A TRUE BUSINESS CONTINUITY PLAN IS VERY DIFFERENT FROM A DISASTER RECOVERY SOLUTION"

Whether you had a documented plan or not, a good approach is to create a small group or task force, and write down your answers to the questions below while the transition is still fresh in your mind.

BUSINESS CONTINUITY PLANNING

Do you have a documented business continuity plan?

If not, determine whether this can be created in-house or if you need the help of a third-party consultant. It's simply a fact that disruptions will happen again and you need to be prepared.

Did your business continuity transition go as planned?

If not, how and why? How could different continuity team members or planning processes have helped make a smoother transition?

What would have gone differently, if anything, in a different type of crisis?

Think about future disruptions, such as a severe weather emergency or a building fire. While very few of us were prepared for a global pandemic, there are procedures you can put in place to smooth transition in the face of an emergency – document those and compare them against other possible crises.

Did your business continuity plan and practice sessions from prior to the disruption match the reality?

Note at least two ways you would improve your plans. Also consider running "surprise" work-from-home drills, just as would do for fire safety.

TECHNOLOGY INFRASTRUCTURE

This is an important area to document before you forget the pain of the first few weeks of your entire staff working from home. As an example, at Ntiva we have a very extensive business continuity plan in place that is tested regularly.

However, we had not fully expected the flood of voice calls we would get for technical support. The barrage of clients who desperately needed help for the sudden transition to remote work meant that we had no phone circuits remaining for our internal audio conferences.

A fast switch to an alternate solution (Microsoft Teams) solved the problem, but you can see how planning for every scenario can be challenging. Take stock of the things that blindsided you.

Did your standard-issue computers support your employee's ability to work from anywhere?

If not, adjust your procurement specifications and budget appropriately. You might want to consider transitioning to laptops where it makes sense, and making sure every employee has a webcam as well.

TECHNOLOGY INFRASTRUCTURE

Did you require physical phones for newly remote employees or did you have a good alternative?

Consider whether or not you had appropriate systems in place, such as call forwarding to mobile phones or soft phones, or if you need to consider an alternate solution. There are many cost-effective Unified Communications (UC) solutions that can provide you with a more flexible arrangement.

Were employees able to remotely access all of the company applications, services and data?

A majority of companies today take advantage of cloud services such as Microsoft Office 365, Salesforce, etc., but many discovered that employees were unable to access data on their internal servers. Consider whether this is the time to migrate to cloud-based services or a managed data center.

Was your standard core infrastructure ready to cope with the switch?

Many companies were unprepared for the sudden surge in Virtual Private Network (VPN) access or remote-desktop access. They had not secured enough bandwidth to support the increased usage from outside the office walls, so take a look at what your projected needs will be.

Did you have enough software licenses for your collaboration platforms such as Zoom, Microsoft Teams, WebEx, etc?

This was another area that many were not prepared for. It's relatively easy to scale the number of subscription licenses you buy up and down, but you may want to prepare from a budget perspective.

Was home bandwidth a problem for all those video conferencing calls?

If working-from-anywhere becomes a standard practice, and you should expect it will, you need to ensure workers are aware of the need for reliable bandwidth, a secure connection, and the necessary equipment as mentioned above.

COMMUNICATION & COLLABORATION

Employees are likely far more comfortable now with video conferencing apps such as Zoom and collaboration tools such as Microsoft Teams and Slack for conducting business.

Many companies pivoted very quickly to increased communication, both internally and externally, with surprisingly results – both positive and negative!

Capture and expand on what went well, and double down on your newfound expertise and efficiency now before old routines reassert themselves.

"DOUBLE DOWN ON YOUR NEWFOUND EXPERTISE AND EFFICIENCY NOW"

What were the hallmarks of your most effective remote work employees?

Conduct interviews with your star players to capture their tips and tricks and then integrate them into broader staff training. This is especially useful for new hires as they start to come on board.

COMMUNICATION & COLLABORATION

What about your managers?

What did these folks put in place and/or do differently to keep productivity and morale high? Document the most successful practices and share appropriately.

Conduct an internal survey to determine the effectiveness of new tools that were suddenly being used.

Was Microsoft Teams an invaluable tool, or did it become a source of constant interruption through the chat feature? Was Zoom so invaluable for team communication that you might consider purchasing more licenses? Did workflow tools such as Asana play a critical role? Most importantly, think about what platforms you want to standardize on, so you don't have different groups of employees using different tools.

Did you increase your daily check-ins, planning meetings and other internal group huddles?

Assess whether you think you should continue this increase of communication, or whether they could be moved to a more informal and real-time method such as chat on Teams or Slack. Did you feel a need to constantly check in on productivity of your remote workers? If yes, you might look into time tracking software.

How quickly and effectively did you communicate with customers, business partners and other stakeholders?

Rate your own effectiveness, but also seek honest feedback via survey or verbal check-ins with external groups. How could you perform better next time?

CYBERSECURITY & RISK MANAGEMENT

A global crisis turns out to be a lucrative playground for cybercriminals. This has worsened with the shift to working from home, where the protective mechanisms that safeguard office networks do not exist.

Stressed employees fell for endless phishing scams, made worse by using computers and other personal devices that were not properly secured, and often over unsecured home networks to boot.

Did all your employees have standard-issue computers that they were able to take home?

Company-provided laptops can be kept much more secure when they are managed by an IT team (in-house or outsourced) vs. letting workers use home computers. Keeping operating systems and other software up to date is crucial, and this can only be done if you have remote management capabilities.

Do you have a Bring-Your-Own-Device (BYOD) policy in place?

Most companies let workers access email, files, and other data from their personal mobile devices. As part of any good security posture, you may want to consider a written policy that outlines the responsibilities of both the employer and the users, including what they can do with their own equipment vs. company owned.

CYBERSECURITY & RISK MANAGEMENT

Are employees trained to save company data in a central and secure place?

It's easy for employees to hit "save" on a document to their desktop. If their computer crashes or gets infected, you've lost potentially valuable data. Whether you use a VPN to connect to a server in the office or take advantage of cloud storage, be sure employees understand the company policy.

Have you deployed Multi Factor Authentication (MFA)?

There is no way around it, you need to protect Internet-acessible systems with MFA – passwords are no longer enough to keep the hackers out.

Are you familiar with identity and access management?

Now more than ever it's important to manage who has access to what, to protect your data from unauthorized access. Consider taking an in-depth look at your existing profiles.

Do you offer regular security training?

There has been an alarming rise in phishing attempts, even pre-Covid-19. You may want to roll out phishing prevention training on an ongoing basis – untrained employees are your greatest weakness.

Have you considered additional security protection for your new remote working environment?

Unfortunately, anti-spam and anti-virus software is no longer adequate protection against sophisticated hackers. Advanced security solutions should be considered – take the time to get an unbiased assessment of your current security posture.

PROCESSES & AUTOMATIONS

Review what business processes and workflows functioned well under the strain and what did not

As an example, we've worked with many companies who until recently were requiring paper invoices that could be stapled to paper purchase orders and paper checks. Manual processes such as these would have become far more difficult during the recent disruption.

There may be many legacy habits that for some reason have never been changed and are incredibly inefficient when compared with newer digitized solutions.

What operations and processes became less efficient, more frustrating, or almost impossible?

Now would be a good time to consider digitizing outdated or manual systems and processes. As a counterpoint, are there any processes that, thanks to the recent disruption, you've realized don't add any value at all? That is, you were unable to do them and no one even noticed their absence. In short: Don't bring all your old baggage back to the office with you.

PROCESSES & AUTOMATIONS

What automation could have enhanced your operations and eased your work-from-home transition?

Where did your people struggle remotely that, in a perfect world, could have been done by an application or other technology – freeing your teams to spend time on value-added efforts and direct customer interactions?

Use your newfound clarity to adjust any outdated processes for the better, including bringing in outside expertise to educate you on how technology could automate your rote processes and/or provide fewer & more time-efficient touchpoints between staff members, suppliers and customers.

What departments, if any, were suddenly over-taxed with the quick shift to remote work?

One of the most obvious was the IT department. Many were completely overwhelmed trying to support the hundreds, if not thousands, of end user requests.

Now more than ever companies are relying on the IT department to lead their digital strategy, their remote work strategy, cyber security challenges and so much more.

Consider whether outsourcing certain areas of IT might be more efficient and cost-effective, especially commodity services such as network monitoring, software upgrades, equipment procurement and even help desk support.

"USE YOUR NEWFOUND CLARITY TO ADJUST ANY OUTDATED PROCESSES FOR THE BETTER"

KEY TAKEAWAYS

There are many things you can do to put yourself in the best position for future growth and success, but here are what we feel are the top considerations when it comes to technology investments.

Start from a secure foundation.
There is nothing more important than cybersecurity protection. Small to mid-sized businesses face a huge risk from cyber threats, so it's imperative that you approach any technology investment with security in mind. Work with appropriate parties to understand your security policies, and how to build the strongest, layered defenses from the ground up.

Focus on resiliency.
While it might feel tone-deaf to say, "never waste a good crisis," it is important to learn from and adapt to disruptions. This includes documenting your successes and struggles for future considerations, as well as considering whether you re-instate inefficiencies that might be better left in the wake of the recent crisis.

Looking to the future, are there any opportunities to increase your customer relationships and market share with some of your lessons learned? The answer is almost certainly yes. By freeing up your team with automation, software and other technology solutions, they can spend more time focusing on growth planning for future success.

KEY TAKEAWAYS

Get team buy-in.
New technology can definitely impact successful growth, but it's only as powerful as the people who use it. Be sure to seek feedback from your executive team as well as other key stakeholders on why certain decisions are being made. Once new tech has been implemented, regular and thorough training should be conducted so that you and your employees get the most out of the investment.

Ask for help when and where you need it.
Many businesses don't have the expertise to address IT security or other complex tasks. Lean on your technology partners, IT consultants and other trusted third parties who can help you choose, customize and implement the right solutions in the most cost-effective manner.

Capital preservation is always critical, but with that said, there are always new technologies that can actually maximize your growth potential and increase your profitability.

Learn more here about the technology services and solutions that Ntiva can provide for your business.

Ntiva
Managed IT, Security, & Cloud Services