IRON MOUNTAIN®

SMALL BUSINESS CONTINUITY PLANS MUST EVOLVE FOR THE POST-COVID WORLD

Few enterprises—let alone small businesses—have continuity plans in place to fully prepare for the incredible disruption of a global pandemic. While you begin to adapt your business to the new reality, it's a good time to review lessons learned from COVID-19.

Crisis management experts say an important part of any disaster response is to take note of gaps or shortcomings and address those while things are still playing out. To help keep track of details, it's a good idea to keep a journal that can inform business continuity plan improvements.

HOW TO APPLY 8 LESSONS LEARNED FROM COVID

1. PREPARE TO SUPPORT MORE REMOTE EMPLOYEES

During the pandemic, many employees have been forced to connect to business networks from home computers that lack company-sanctioned software, up-to-date malware protection, encryption controls and secure email applications. Security risks have been amplified by the need for some employees to share computers with roommates and children. To help alleviate these issues, consider providing all employees with preconfigured company laptops for home use.

2. STOCK A SHARED POOL OF LAPTOPS

If you're unable to provide everyone with a laptop, you can stock a pool of laptops to be assigned out as needed. If that isn't possible, get key information about personal laptops ahead of time, including employees' media access control (MAC) and IP addresses. Give employees detailed instructions for downloading and installing the software they need securely.

3. ENSURE EMAIL RESILIENCE

Most of us feel lost without a remote access option to work email. Luckily, nearly all email services today are cloud-based or have a browser-based "webmail" option. However, the few employees who may not have access to your company's approved email server should know alternative means of access. They should also be warned not to forward business email to a personal account, which may lack the security and auditing features your business needs.

4. REVISIT BUSINESS CRITICAL OPERATIONS

Perform a deep-dive analysis on your small business operations before a crisis even begins. Decide what functions are essential and what functions can downshift into low gear. This could include anything from internal operations like equipment maintenance, security, janitorial services and IT support as well as external operations like field service.

5. DEVELOP A SKILLS BACKUP PLAN

During the first weeks of the pandemic, healthcare organizations were swamped with calls to their contact centers. Many had to shift employees from other departments into customer service. How would your organization handle a situation that caused a sudden spike in demand or that took key people out of their assigned job? Consider building an in-house job bank with a skills inventory of your entire team so the right people can be tapped to plug emergency gaps.

6. REVIEW YOUR SUPPLY CHAINS

The pandemic revealed a painful flaw in inventory management. Many retailers and manufacturers were caught off guard when their suppliers were shut down by COVID-related illnesses and government mandates. Businesses need to revisit their supply chain plans with a greater emphasis on resiliency measures that include secondary suppliers and larger inventories.

7. PLAN FOR DISTRIBUTED DATA BACKUP

Typically, in-person employees take data backup for granted. When they occasionally work from home, the need for backup may not even occur to them. Many of the 200 million monthly users of Office 365 probably aren't aware that there is no automatic backup. Years before COVID, backup started becoming an increasingly mission-critical function due to the steep increase in ransomware attacks.

There are services like Carbonite's cloud backup solution, which runs transparently in the background, to provide end-to-end encryption of data over a secure connection. Iron Mountain's strategic partnership with Carbonite enables our Iron Cloud customers to provide backup smoothly for employees as they work onsite and remote.

8. GIVE EMPLOYEES A CRASH COURSE IN INFORMATION CYBERSECURITY

Phishing attacks, which attempt to trick users into clicking on malicious links in legitimate-looking emails, have exploded during the pandemic. When people are hungry for information, they let their defenses down. There has also been a huge increase in the use of cloud-based file-sharing services and collaboration applications, which can create vulnerabilities if they aren't monitored.

To help navigate and avoid scams during a time of crisis, create a work-from-home security checklist for your remote employees that covers how to access authorized software and services with sufficient security and avoid unauthorized activity. This is a great place to start building out a tailored company information cybersecurity crash course to prepare for the next crisis.

REMEMBER...

In times of crisis, there are usually seeds of opportunity. Small businesses that apply lessons learned from COVID-19 will emerge with new insights into their operations and be better prepared to survive future shocks to the system.

To help get the ball rolling, Iron Mountain has a full suite of secure digital information management solutions that include:

- Document digitization
- Cloud storage with fast retrieval
- Document workflow automation

To learn more, go to: ironmountain.com/smb

WHY IRON MOUNTAIN?

- Bestselling SMB Solutions
- Dedicated account representatives
- 24/7 Customer Service