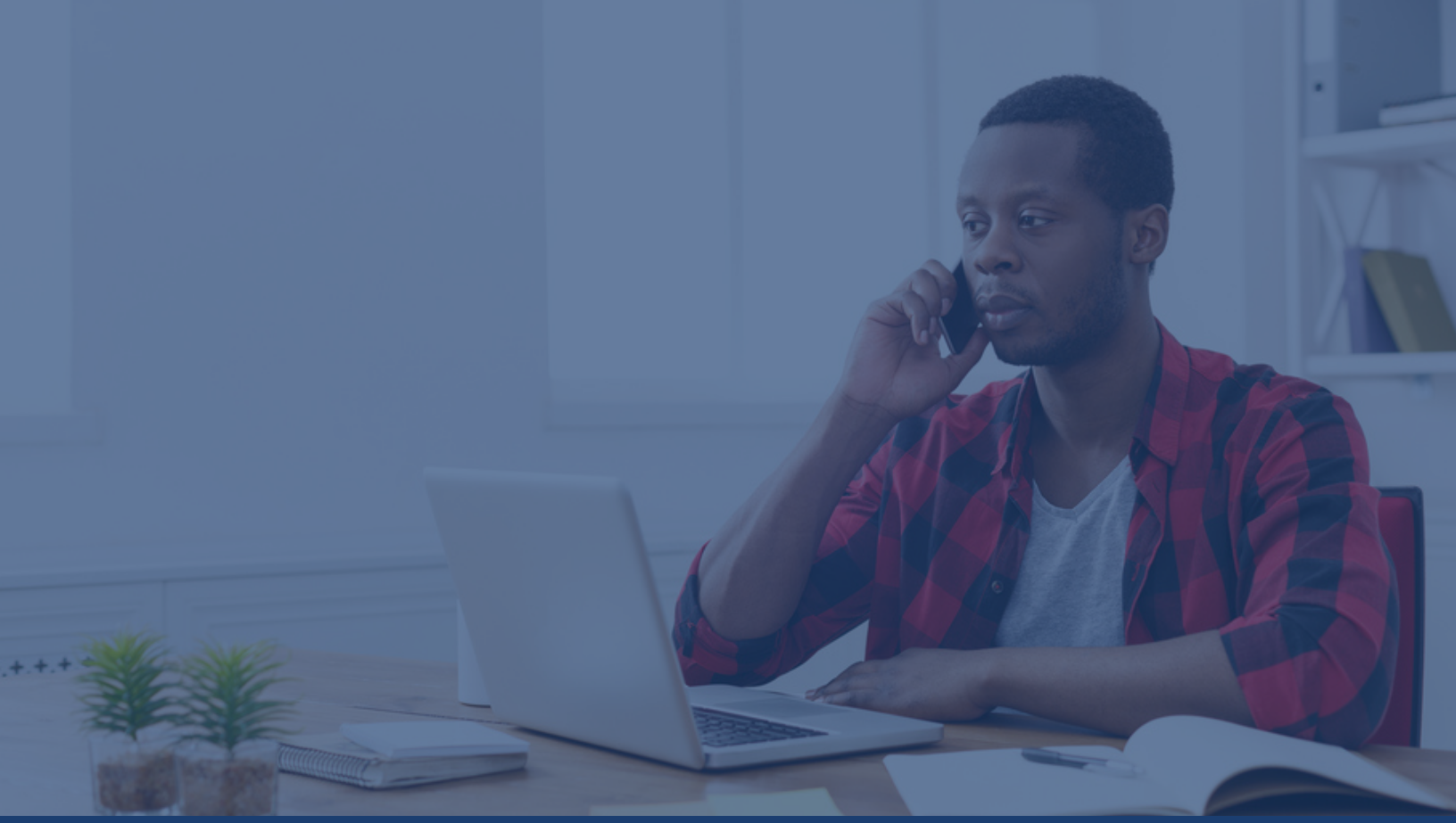

WHITE PAPER

IT STRATEGY FOR POST-COVID ERA

Before and after Covid-19

RKON
PRIVATE EQUITY SERVICES

Given the complete transformation in business operations over the last few months, it's critical to employ quick responses, proactive plans, and resilient security measures to protect employees and assets.

Here are the biggest changes we've seen as organizations continue to combat Phishing, Data Breaches, & Business Email Compromise:

OFFICE

- On-Premise Solutions
- Corporate-issued
- Devices
- Internal Network

HOME

- Cloud-Based Solutions
- Personal
- Devices
- VPN Usage

RECOVERING FROM A DISASTER

If businesses were unsure about their disaster recovery plans before, COVID-19 has certainly demonstrated the unmistakable need to implement disaster recovery and business continuity plans that can sustain business operations, even in the face of a global pandemic. While it's not often that businesses are confronted with natural disasters and global pandemics, the need for updated, proactive disaster recovery plans is more urgent than ever.

No business can survive a pandemic like COVID-19 completely unscathed; however, with the right preparations, businesses can be ready for the unthinkable, which could mean the difference between life and death for your operations during a disaster.

LIMITING THREATS, NOT EMPLOYEES

The uptake in remote work has forced a huge strain on IT infrastructure. Remote workspaces either completely lack the proper security measures needed to keep employees safe, like VPNs, or IT systems are struggling to keep up with the significant surge in devices connecting to corporate networks. Not to mention, employees often prioritize productivity over security, bypassing corporate VPNs to access cloud services or using personal devices over corporate-issued devices, thereby lacking proper security controls.

It's no question that COVID-19 has caused a major shift in IT departments. Before disaster recovery scenarios were prepared for internal attacks, outsider threats, failing equipment, and human error, but now, companies are adding to this list viral pandemics, power outages, tornadoes, floods, data centers shutdowns, and more. If there's one thing that COVID-19 has taught IT, it's that no matter what the scenario, disaster recovery, and business continuity plans must be updated, standardized, clearly communicated, and regularly practiced in order to ensure seamless processes and protection amidst real-life havoc.

5 SECURITY TIPS FOR THE POST-COVID ERA

1. COMMUNICATION

Clear communication is an essential part of keeping operations running smoothly and without disruption. Since COVID has forced employees to step away from face-to-face communication and embrace virtual conversations, it is crucial for businesses to have transferable equipment and a concise, step-by-step plan for employees to make sure everyone knows their role moving forward.

2. INSPECT ENDPOINTS

Once you've established a clear disaster recovery and business continuity plan and communicated it with employees, it's vital to inspect endpoints connecting to the corporate network computing. This ensures that employee devices are up-to-date on all policies and gives visibility into each endpoint that requests access to internal resources and whether they're meeting necessary requirements

3. LEVERAGE THE CLOUD

Cloud-based SaaS offerings, including multifactor authentication (MFA), network firewalls, antivirus, threat management, URL filtering, and more, are equipped to manage a number of remote work threats, keeping your business safe from the influx of phishing attempts that have taken advantage of remote working environments.

4. ESTABLISH BACKUPS

Having a second storage location for your data, such as virtual infrastructure or cloud backups, provides a clear advantage to businesses when trying to protect their data from threats. Recovery for local files might be faster, but the cloud provides a safe off-site location in the event of a data center disaster.

5. INVEST IN SECURITY

In the post-COVID era, don't be afraid to ramp up your security controls, especially now that remote work has made employees more vulnerable to breaches. Creating USB lockdown policies, investing in email cloud services like Mimecast, or employing SIEM tools like Rapid7 could make or break your security posture in the era of remote work.