US SIGNAL

A DR PLAN Checklist

If a disaster were to affect your IT operations, are you confident that your company would be ready? If you answer "no" to any of the questions that follow, you may want to consult with a third-party company that specializes in DR solutions.

A good place to start is US Signal. US Signal can assess your DR preparedness, enhance your current DR plan or devise a customized one.

Call 866.2.SIGNAL or email us at: info@ussignal.com.

THESE FIRST 12 QUESTIONS APPLY WHETHER YOU HAVE A DR PLAN IN PLACE OR ARE CONSIDERING ONE.	Y	N
1. Have you conducted a business impact analysis to determine the operational, financial and reputational effects to your business if your IT assets were not available?	○	○
2. Have you calculated the direct and indirect costs of downtime to your organization?	○	○
3. Do you have an inventory of your IT assets, such as hardware, software, data and applications (including any that may have been introduced due to "shadow IT")?	○	○
4. If you have an IT asset inventory, does it include application and system dependencies?	○	○
5. Have you determined which of your IT assets are most critical to keep your business operating if a disaster strikes?	○	○

	Y	N
6. Are there any compliance or other requirements associated with your data or applications that may affect a DR plan?	○	○
7. Have you established RPOs and RTOs for your data and applications?	○	○
8. Do you currently back up your data and applications?	○	○
9. Are your backups kept off-site?	○	○
10. Do you replicate your data?	○	○
11. Have you conducted a risk assessment, or at least compiled a list of all the various disaster scenarios that could affect your company - including ransomware or other cyberattacks, as well as natural disasters?	○	○
12. Does your organization use the 3-2-1 rule for backups?	○	○

THE FOLLOWING 12 QUESTIONS APPLY IF YOU HAVE A DR PLAN.	Y	N
1. Is your DR plan tested at least once a year?	○	○
2. If your DR plan is regularly tested, does it also get updated based on the results?	○	○
3. Does your company maintain regularly updated runbooks that detail your DR processes and procedures?	○	○
4. Is recovery and protection possible at the application level?	○	○
5. Is your DR plan resilient and are you confident your company can continue operating even if a disaster strikes?	○	○

	Y	N
6. Does your team have the training necessary to fail over a site?	○	○
7. Do you currently have a hot, cold or warm site or use the cloud to minimize downtime and data loss?	○	○
8. If you aren't using cloud-based DR, are you content to continue allocating resources and budget money to purchasing, managing and maintaining your DR infrastructure?	○	○
9. If you aren't using cloud-based DR, are you confident that you're staying up to date with the newest DR technologies?	○	○
10. Does your DR plan meet all your compliance requirements?	○	○
11. Does your DR plan include measures to help ensure your backups don't contain ransomware or other malware?	○	○
12. If you're using a third-party Disaster-as-a-Recovery (DRaaS) solution, are you satisfied with the SLA in terms of restoration time, infrastructure availability and other key criteria?	○	○

NOTES: