GRADE·A

CORPORATE DATA BREACH

# 5-STEP RESPONSE CHECKLIST

## ☐ REMOVE IMPACTED DEVICE FROM NETWORK

As soon as you have confirmed that a data breach has occurred within your IT infrastructure, immediately remove any affected devices from the network.

## ☐ CHECK FOR THE LATEST BACKUP

If your business has a data backup process in place, check your system (external hard drive, cloud solution, etc.) for the latest backup date.

If your data was not backed up, you will need to hire professionals to attempt to recover it. Be aware that the data will, in many cases, not be recovered.

## ☐ RESTORE DATA FROM LATEST BACKUP

Restore your data from the latest backup and decipher what data was lost in the breach. Follow the directions provided by your system administration.

Note that restoring a backup won't always provide complete data recovery. In 2018, Commvault found that only 42% of ransomware victims reported being able to fully recover their data from backup.

## ☐ RECOVER SERVER

If your server has failed or been compromised in the breach, take the proper steps to secure and recover it before resuming business.

Never perform server maintenance without the assistance of professional IT support, such as a dedicated IT employee or a managed services provider.

## ☐ PERFORM POST-INCIDENT ANALYSIS

A thorough post-incident analysis should be conducted in order to determine a number of key factors, including:

What data was breached?

What are the appropriate steps to take to recover or protect this data?

Are there any vulnerabilities in the current system that should be accounted for?