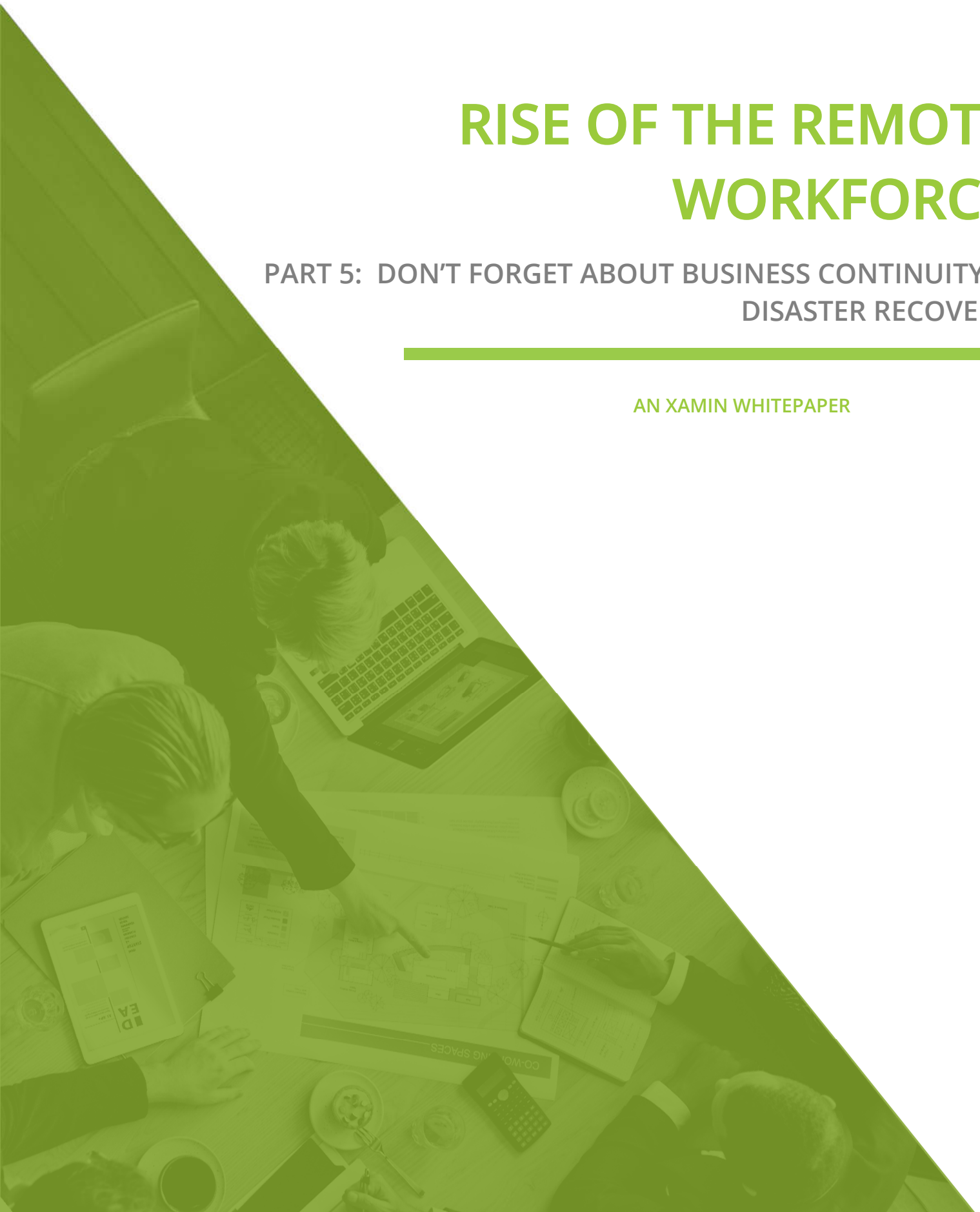
RISE OF THE REMOTE WORKFORCE

PART 5: DON'T FORGET ABOUT BUSINESS CONTINUITY & DISASTER RECOVERY

AN XAMIN WHITEPAPER



The pandemic has changed the way financial institutions (FI) approach their remote workforce and has created a renewed focus on enabling temporary to permanent work from home (WFH) users. Like it or not, remote work is here to stay which puts an onus on the FI to update policies and procedures to protect themselves and their staff. Addressing these changes in the disaster recovery and business continuity (DR/BC) plans will need to be prioritized in order to stay ahead of the auditory guidelines and regulations.

Every year, financial institutions are required to participate in annual third-party audits, many specifically focused on the information technology infrastructure. A component to the annual review process is performing a disaster recovery and business continuity test to verify successful operations of the IT infrastructure at a separate location in the event the institutions primary building was unavailable. In the past, this 'separate location' was typically a branch geographically distanced from the primary operations center or a leased facility through a "bank-in-a-box" provider.

More recently, with the wide availability of secure cloud data protection services, many FI's are beginning to utilize a cloud recovery environment to perform DR/BC testing. This gives the institution an always available recovery solution to perform testing at any point throughout the year without disrupting production.

In 2008, the FDIC released a letter identifying actions all FI's should take to create an effective pandemic policy.

This was one of the primary reasons we (Xamin) started researching cloud recovery solutions around five years ago. Our clients continued to talk about their desire to be able to restore and test connectivity to their solutions and services at any time throughout the year. Investing in building out a physical disaster recovery environment at another location is expensive and adds more potential vulnerabilities to the network. Implementing a cloud data protection and recovery service provides a FI with secure and redundant backup storage while also leveraging cloud recovery. The backup images replicated to the cloud can be powered up and accessed through a secure VPN (virtual private network) connection whenever the institution desires.

What's most unique about this type of solution is the ability to allow employees to connect to the recovery environment from any location with an Internet connection. With a higher percentage of staff working remotely, setting up a DR/BC strategy with connectivity for users that could be located anywhere is a must for all institutions as they look to bolster and expand their recovery plans. While this is an important first step, there's more to enhancing disaster recovery and business continuity

planning than just ensuring all users, be it remote or onsite, can do their jobs when disaster strikes.

HOW WELL DID THAT PANDEMIC PLAN WORK?

"Wow, who would have thought we'd actually have to use this thing!"

Back in 2008, the FDIC (Federal Deposit Insurance Corporation) released a letter identifying actions all financial institutions should take to create an effective pandemic policy. Because the financial space is highly regulated, most institutions have some version of this policy which is reviewed and audited annually. The scenarios laid out in these plans have typically been around cross-training staff to deal with the loss of employees and a strategy to ensure the continuance of business operations. While effective to a degree, one of the primary issues we experienced with some of our clients is how prepared the institution was to scale this plan.

Comprehensive disaster recovery and business continuity policies document the process for which an institution will follow in the event the primary operations center is unavailable, but rarely do they consider an event such as the current pandemic where primary operations are still functioning, but the majority of employees are not in physical offices. Remote connectivity and mobile computing are typically structured into the annual testing scenarios but have historically been for a select number of critical staff or executives. Going forward, these policies will need to include plans for scaling up to service the entire workforce. During a global pandemic hardware is more difficult to procure and technology resources needed to deploy solutions quickly can be busy and overworked, so it's important these considerations are made now and the plan is updated accordingly.

While your financial institution may have enacted a successful rollout of your disaster recovery and business continuity procedure, recent events have shown us there are other aspects to pandemic planning that must be considered. Cross-training staff is an effective way to combat the temporary loss of employees, but dealing with where those employees are working from, what they're working on and how they're connecting to the institution's environment are all crucial components to consider. In addition, if the institution has more remote workers and a loss of the primary operations center was to occur, having an effective recovery solution for the entire workforce will become high priority. Perhaps the most important reminder from all of this is it's imperative you don't forget about business continuity and disaster recovery testing.

Xamin has helped financial institutions for over 20 years align goals & people with the right technology, security, policies, and best practices.

ABOUT XAMIN

Together With You.

We've gained the trust of organizations across the country by going above and beyond. Our process aligns your goals & people with the right technology, security, policies, and best practices.

Schedule a call with our CEO & Technology Specialists

Infrastructure | Security | Data Protection
Cloud | Professional Services

1-844-44XAMIN
www.xamin.com

xamin