CHAPTER

5

Disaster Recovery

Scott R. Ellis and Lauren Collins
kCura Corporation

1. INTRODUCTION

In almost every organization, when a technology-oriented task is at hand, and where no one knows who would handle the request, it typically lands in the information technology department (IT). Whether the task consists of a special, faulty light bulb or a backup for a grease stop in the kitchen sink, organizations rely heavily on the IT department to know the unknown, and to fix anything that breaks.

Disaster recovery (DR), not unlike the plugged sink, is another task that many organizations fail to consider until after much of the technology groundwork has been laid, the corporation is profitable, and suddenly someone realizes that *not* having a DR site is a serious risk to the business. It is at this time that they begin to consider, and they begin to ponder, what a strategy might look like that enables the business to continue to run in the event of Force Majeure or some other disaster, such as if a hacker came in and tore their system down, or somehow seized control of it.

Hardware, physical or virtual, must be acquired and configured to capture the environment as it currently sits—and it must be able to continue with its synchronization. Whether this is by the minute, the hour, the day, or the week is a business decision. In fact, much of the DR strategy is driven by business continuity requirements. In the event of a disaster, there must be a plan in place that considers which individuals will act in the event of a disaster. Those individuals must know what constitutes a disaster, and the roles must be defined for those individuals.

2. MEASURING RISK AND AVOIDING DISASTER

A key component of a disaster recovery (DR) plan is for the committee to assess conceivable risks to the organization that could result in the disasters or emergency situations

Cyber Security and IT Infrastructure Protection
DOI: http://dx.doi.org/10.1016/B978-0-12-416681-3.00005-7