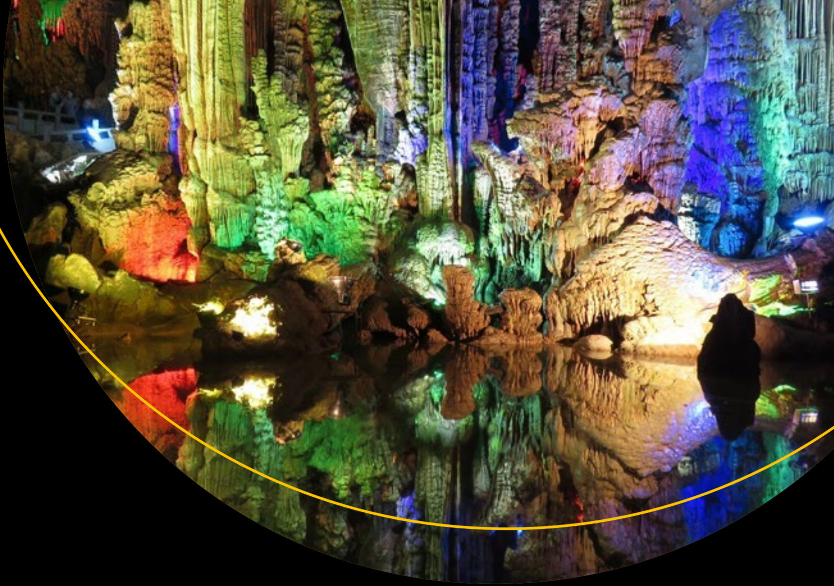

IT Disaster Response

Lessons Learned in the Field

Greg D. Moore

Apress®

IT DISASTER RESPONSE

LESSONS LEARNED IN THE FIELD

Greg D. Moore

Apress®

IT Disaster Response: Lessons Learned in the Field

Greg D. Moore
Brunswick, New York
USA

ISBN-13 (pbk): 978-1-4842-2183-9 ISBN-13 (electronic): 978-1-4842-2184-6
DOI 10.1007/978-1-4842-2184-6

Library of Congress Control Number: 2016961531

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Developmental Editor: Laura Berendson
Technical Reviewer: Thomas Walsh
Editorial Board: Steve Anglin, Pramila Balan, Laura Berendson, Aaron Black,
Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John,
Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie,
Natalie Pao, Gwenan Spearing
Coordinating Editor: Rita Fernando
Copy Editor: Kim Burton-Weisman
Compositor: SPi Global
Indexer: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary materials referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book’s source code, go to www.apress.com/source-code/.

Printed on acid-free paper

Apress Business: The Unbiased Source of Business Information

Apress business books provide essential information and practical advice, each written for practitioners by recognized experts. Busy managers and professionals in all areas of the business world—and at all levels of technical sophistication—look to our books for the actionable ideas and tools they need to solve problems, update and enhance their professional skills, make their work lives easier, and capitalize on opportunity.

Whatever the topic on the business spectrum—entrepreneurship, finance, sales, marketing, management, regulation, information technology, among others—Apress has been praised for providing the objective information and unbiased advice you need to excel in your daily work life. Our authors have no axes to grind; they understand they have one job only—to deliver up-to-date, accurate information simply, concisely, and with deep insight that addresses the real needs of our readers.

It is increasingly hard to find information—whether in the news media, on the Internet, and now all too often in books—that is even-handed and has your best interests at heart. We therefore hope that you enjoy this book, which has been carefully crafted to meet our standards of quality and unbiased coverage.

We are always interested in your feedback or ideas for new titles. Perhaps you'd even like to write a book yourself. Whatever the case, reach out to us at editorial@apress.com and an editor will respond swiftly. Incidentally, at the back of this book, you will find a list of useful related titles. Please visit us at www.apress.com to sign up for newsletters and discounts on future purchases.

—The Apress Business Team

This book is dedicated to Duke Moore,
my father, the strongest man I've ever known.
He taught me integrity, standing up for what
one believes in, and going the extra mile. He also
taught me my first puns and gave me a love of
reading and writing. He had always wanted to
write the Great American Novel.

Dad, I never could get you into a cave,
but I can get you into a book. I just wish you were
around to read it. It's not the Great American Novel,
but I think you'd like it anyway.

Contents

About the Author

Greg D. Moore has been both an independent consultant (Green Mountain Software and the founder of QuiCR, LLC) and a director and later VP of IT at several internet startups that had 24/7 requirements. In both roles, much of his focus has been as a DBA. However, he has experience with networking as well as recent experience with programming. His blend of hands-on technical skills combined with his management skills gives him a unique insight into disaster planning. He has helped clients through disasters, as well as helped develop and test disaster plans, and experienced a few of his own.

Greg is also an instructor with the National Cave Rescue Commission (NCRC) and the Northeast Coordinator for the NCRC. He has participated in a several cave rescues, across four states, and has helped train hundreds of cavers and emergency responders across the United States and Puerto Rico.

About the Technical Reviewer

Thomas Walsh started his career in Emergency Medical Services in 1986, which grew from a college emergency squad to the director of clinical services for a local emergency medical services agency. He has experience as a volunteer firefighter, EMT, and paramedic in a variety of urban and rural health care systems. Tom has spent many years as a helicopter flight medic, where he gained significant insight into the aviation safety culture and high-stakes environment of critical care medicine. Tom is passionate about the education of new providers, health care system management, aviation, and health care safety. A prolific educator and lecturer, he is always exploring and studying human performance during critical events with zero-fault tolerances and high levels of stress.

Tom holds a Bachelor's of Science in Health and Biology from Excelsior College, received his paramedic training from Sand Hills Community College in Pinehurst, NC, and is a Certified Medical Transport Executive. Currently, he resides in the Albany, NY, area with his wife, Christine, and his daughter Emily, working as a paramedic clinical educator. Tom is a member of the adjunct faculty at Hudson Valley Community College paramedic program. He has a keen interest in aviation, health care, EMS, information management, space flight, gardening, and many outdoor activities. Yes, Greg has dragged Tom into a cave to practice the rescue of an injured caver.

Acknowledgments

First I want to acknowledge the IT teams I have had the honor and pleasure of managing over the years. We made it through Y2K and many other incidents together.

Second, I want to thank my fellow NCRC instructors and coordinators. You literally wrote the book on cave rescue. I'm proud to be among your numbers. I've learned a lot from cave rescue and hopefully have been able to apply a few of the lessons learned to here.

I would like to thank Tom Walsh, who has been a great sounding board and editor. Without your input and corrections, this book wouldn't be what it is today.

Finally, I want to thank my wife, Randi, and my kids, Ian and Rebecca. You've been a great support and my world would be less fulfilling and less beautiful without you.

Introduction

I grew up in a former railroad station, across the street from a firehouse, and one of my favorite shows was *Emergency!*. These may seem like incongruent facts, but they actually helped shape me in a number of ways.

I would watch as the firefighters would race to fires and would often discuss with my classmates the most recent big fire in town. While I was too young to join the fire department and moved away before I could become officially involved, I always had a great deal of respect for what they did. I recall when they upgraded from an ambulance that was essentially an oversized station wagon to an actual van that today we would recognize as being closer to what we think of as an ambulance. Later they upgraded again to what would definitely today be recognized as an ambulance. I didn't fully understand the changes. It was only years later that I realized that the training and tools were evolving. Early ambulance drivers were often the guys (and back then, most were men) that could drive the patient to the hospital as quickly as possible. Many were actually morticians. This was because many ambulances were basically hearses. If you think about it, a coffin and a litter both slide in the same way.

There wasn't much more requirement than driving fast. Over time, the EMS community emerged with the earliest EMTs and paramedics. People that previously would have died before they could get to the hospital were receiving treatment in the field that only a decade before was not possible.

Much of this was mirrored in the TV show *Emergency!* It wasn't until decades later I realized how much of an impact *Emergency!* had on the industry. There are many EMTs and paramedics today that say they got into the field because of that show. But *Emergency!* was more than just a TV show. It was almost a documentary based on a very famous paper written in 1966—now called "The EMS White Paper." Its more formal name is "Accidental Death and Disability: The Neglected Disease of Modern Society."[1] This paper revolutionized how we think about emergency medicine.

The history of railroads doesn't necessarily have a single seminal event like that white paper. But it is often said that the rules of railroads are written in blood. This means that basically every rule is there as a result of someone dying and the rule being put into place to prevent future such deaths.

[1] https://www.ems.gov/pdf/1997-Reproduction-AccidentalDeathDissability.pdf

One example is what is known as blue flag/signal protection. Simply put when equipment is being worked on, or for passenger trains, cars or locomotives being added or removed, a blue flag or signal is placed in such a way to warn all other workers that movement of the train or car in question could cause a serious injury or death. There's an additional detail to this rule that is important. A blue flag/signal may be placed by a member of one of the repair crafts. The important part is that it may be removed *only* by the same person who placed it or a member of the same craft. (Here *craft* is perhaps best defined as people in the railroad with similar job functions or skills.)

This detail on who may remove it is important because in part it means people with the same skills and knowledge and the ones in the best position to know if it is safe to move the car or train are protecting each other. It also means that for example an engineer or conductor, or even in theory the CEO of the railroad, cannot remove the blue flag/signal protection. Just because they may be considered to have a higher job position, that position doesn't give them the authority. Keep this in mind later in the book as we discuss things like the Incident Command System and Crew Resource Management.

So what does all of this have to do with a book on IT disasters? Good question. While I grew to love computers at an early age, I also grew to love understanding how disasters unfold and how we respond to them. Just as the EMS field and railroads have matured over time and introduced new best practices, and if necessary, removed outdated practices, so has the IT field.

Over time, we've learned better ways to respond to disasters—and equally important, how not to respond.

As I grew up, I started to get more involved in various outdoor activities, including caving. In 1999, I took my first class on cave rescue and I became hooked. I also took lessons from that course, specifically ICS, and applied them to our Y2K response six months later.

This book then is a result of my watching EMS evolve, learning how railroads worked, cave rescue, and more, and applying the lessons learned to IT.

I've enjoyed writing it and I hope you enjoy reading it. And hopefully, you learn something from it.

CHAPTER

1

A Different Approach

There are many books out there written for disaster planning in the IT world. Most focus on very specific ideas or concepts, such as developing a backup strategy for on-site and off-site storage of critical data. Some books talk about developing and writing a disaster response (DR) plan. This isn't exactly one of those books.

Although there are some examples in this book and hopefully some useful takeaways, this book is more designed to make you think about how to approach a disaster, not the specific steps to take during a disaster. I will avoid the obvious things like, "make sure you do backups" (though you should).

For the most part I'll be using "We" in this book because though it's sort of a one way forum, I sort of see this as a journey we're taking together.

This book draws upon a diverse set of ideas and experiences—not all immediately associated with DR in the IT workplace. However, hopefully by the time you get done reading you'll see the relevance. And hopefully you'll have had some fun and learned something. Yes, I did say *fun*, because if you're not enjoying your job, my advice right now is to start looking for a new job and find one you do enjoy. I can safely say, overall, I have fun at what I do and I'm having fun writing this book.

G. D. Moore, *IT Disaster Response*, DOI 10.1007/978-1-4842-2184-6_1

My background is primarily in the IT space. I've worked with computers professionally for over 25 years. I've helped write DR plans, test them, and in a few cases, implement them. I've also had to deal with disasters where there was no formal DR plan and we had to go by the seat of our pants. Most of those were successful, some weren't.

When I'm not found behind a keyboard I can often be found either caving or teaching cave rescue techniques. I'm currently the database administrator for the National Cave Rescue Commission and the Northeast Regional Coordinator. I'm also an instructor. This background has given me some unique thoughts about DR plans and some cross-domain knowledge.

I'm also an avid reader that reads across a number of disciplines and enjoy reading about how we think and process. Check out my blog at `https://greenmountainsoftware.wordpress.com`.

All of this comes into play in my DR thoughts and my ideas in this book.

What Is a Disaster?

> *"But I know it when I see it."*
>
> —Justice Potter Stewart

Sure, you may know a disaster when you see it, but sometimes it helps to have a working definition. For the purpose of this book, I will be using the following definition:

> Disaster: An unplanned interruption in business that has an adverse impact on finances or other resources.

This is purposely a rather broad definition so let's discuss it a bit and be clear about what I mean.

Your facility is struck by a truck and catches fire. The server room is destroyed in the resulting explosion and fire-fighting effort. That's pretty clearly a disaster. I don't think anyone would really quibble over that.

Your server is running fine one day when the power supply dies and you can't reboot it. That example is perhaps not quite as dramatic, but still a disaster.

Your printer runs out of paper and displays the dreaded [PC LOAD LETTER] in the middle of a report. Yes, this is a disaster using the definition and I quite intentionally include it as such. Sure the impact may be small. It might take you five minutes to reload it and carry on. But that's five minutes of your time you weren't expecting to spend on that. Now what happens if that report is the one the CEO needs in order to present to the board meeting in 15 minutes and now it will be late?

The point is, not all disasters have to be huge. In point of fact, most are not. If you think about it, how many times have you received a call that your data center has burned down versus the number of times you've received a call that a printer isn't responding?

Not all disasters are huge, but some are far more common than others. Any approach to disasters must take that into account. Also, many of the concepts are the same across the board.

I start in Chapter 2 by discussing what a disaster response is and why we even bother having one. This may sound like an obvious exercise, but the truth is, I've encountered companies where the attitude is basically, "eh, we'll deal with it when it happens." Or, they go to the other extreme and have 30-page documents on how to respond to a paper jam. OK, that last one might be a bit of an exaggeration, but it's not far from the truth. I've seen companies operate at either extreme and that's far from ideal. In fact part of the impetus for this book was a client who was planning to purchase hardware for a disaster response solution, but really didn't have a written policy on what would trigger such a response. The hardware was great, but I felt like they were missing something important. This is similar to a company having an *automatic external defibrillator* (AED), but not training employees on when or how to use it. Fortunately, AEDs are easy to use and fairly foolproof. However, the American Red Cross and other organizations still encourage training in how to use them. So simply having the equipment or even a written plan isn't enough if you don't know how to use the equipment or when to implement the plan.

Next, I'll talk about a concept known as the Incident Command System (ICS). This is covered in more detail on Chapter 3, but simply put it is a management structure developed to respond to "incidents" or in our case, disasters. I will often use the term *incident* instead of *disaster* because the connation of a disaster is a huge problem, when really we want to talk about incidents of all sizes.

In Chapter 4, I talk about *crew resource management* (CRM) and its development, and how it has made being a passenger in an airplane much safer than it was and how you can apply similar concepts to your disaster response. I'll drive home the idea of "make sure someone is flying the airplane."

I discuss the role of checklists in Chapter 5: why to use them, when to use them, and when not to use them. Although a checklist is very useful tool, it is not a panacea.

I'll also touch upon the roles of management and IT, and the people you hire or that hired you. This is covered in Chapters 6 and 7. People are a huge part of your disaster response. People with the proper training can make a huge difference in a disaster. We'll touch upon how being flexible in your management structure, especially during a disaster response can be a key factor in a successful response. And hopefully you'll start to look at the individuals in your organization and start to look at their strengths and weaknesses. This may encourage you to hire differently or increase training.

Since I've mentioned that disasters come in all sizes, we'll talk about size: it matters. Chapter 8 covers the small stuff and Chapter 9 the big stuff. We will also discuss how we really want to prevent a small disaster from turning into a large disaster. Pretty much all large disasters start out small. If we can keep them that way, we can make our jobs a lot easier. Chapter 10 discusses when a DR plan is not enough. DR plans are not magical panaceas. Having one doesn't guarantee you'll go through a disaster unscathed or without incident. In fact, I can almost guarantee that the disaster that you do have will have significant differences from what you planned for. However, we'll talk about why a DR plan is still of value. We'll discuss the strengths and limitations of DR plans.

Actual testing is one area that I've found far too few companies invest in. I talk about why this is critical in Chapter 11, as well as the pitfalls of not doing it, or doing it incorrectly.

In Chapter 12, I talk about disaster mitigation and prevention. Here I'm going to make a point that I often see overlooked. Sometimes the answer to preventing a disaster is not to add more hardware or procedures, but rather to simplify things.

And sometimes you can see disasters that are coming up. This may sound like it contradicts my definition of a disaster, but it doesn't. You can expect a disaster, plan for it, and prevent it. You can also expect a disaster, do no planning, and fail to prevent it. Or you can even expect it, plan for it, and still have issues.

In the epilogue, I pull everything together and summarize the journey we've taken together. I also provide a list of suggested reading. This is far from an exhaustive list. I only highlight a number of the books I've read and in some cases referenced in this book. But trust me, there's a *lot* more out there. Some are very specific, such as text books on ICS. Some are books that I myself have yet to read, such as *The Challenger Launch Decision* by Diane Vaughan (University of Chicago Press, 1996); it is a book that has long been on my reading list, but until now, unread.

Each chapter has a similar format. I introduce the concept, and when possible, I give some background, history, and references. Then I show how I apply it to DR planning. Each chapter ends with an actual real-world scenario that either happened to me or that I am familiar with. Finally, I dissect the example and show how the concepts in that chapter, and possibly others, apply.

So let's begin.