APPENDIX

A Disaster Risk Assessment Matrix

For a thorough disaster risk analysis, we recommend ranking the risks facing your organization by using a standardized matrix that accounts for each risk's probability of occurrence and its potential impact to the organization. Table A-1 is a sample risk assessment matrix that both large and small organizations can tailor to the specifics of their systems.

To use the matrix, assess the values appropriate for each of the columns of probability and impact. As we emphasize in Chapter 16, these values are likely dependent on what your organization does, its infrastructure, and where it is located. An organization operating out of Los Angeles, CA, in the US may have a higher likelihood of experiencing an earthquake than an organization operating out of Hamburg, Germany. If your organization has offices in many locations, you may even want to do a risk assessment per location.

Once you've calculated the probability and impact values, multiply them to determine the rank of each risk. The resulting values can be used to order the risks from highest to lowest, which serves as a guide for prioritization and preparation. A risk that ranks 0.8 will likely require more immediate attention than risks that have a value of 0.5 or 0.3. Be sure to develop response plans for the most critical risks your organization faces.

Table A-1. Sample disaster risk assessment matrix

Theme	Risk	Probability of occurrence within a year	Impact to organization if risk occurs	Ranking	Names of systems impacted by risk
		Almost never: 0.0 *Unlikely: 0.2* *Somewhat unlikely : 0.4* *Likely: 0.6* *Highly likely: 0.8* *Inevitable :1.0*	*Negligible: 0.0* *Minimal: 0.2* *Moderate: 0.5* *Severe : 0.8* *Critical: 1.0*	*Probability x impact*	
Environmental	Earthquake				
	Flood				
	Fire				
	Hurricane				
Infrastructure reliability	Power outage				
	Loss of internet connectivity				
	Authentication system down				
	High system latency/ infrastructure slowdown				
Security	System compromise				
	Insider theft of intellectual property				
	DDos/DoS attack				
	Misuse of system resources—e.g., cryptocurrency mining				
	Vandalism/ website defacement				
	Phishing attack				
	Software security bug				
	Hardware security bug				
	Emerging serious vulnerability, e.g., Meltdown/Spectre, Heartbleed				