# Contents

## Part I  The Concept of Anti-fragility

1 **Introduction** ................................................. 3  
   1.1 Complex Adaptive Systems ........................................ 4  
   1.2 Fragile, Robust, and Anti-fragile Systems ....................... 7  
   1.3 Overview of Book ............................................... 7  
   1.4 Creating and Maintaining Anti-fragility ....................... 8  
   1.5 Anti-fragility to Downtime .................................... 9  
   1.6 Anti-fragility to Malware Spreading .......................... 9  
   1.7 Anomaly Detection ............................................. 10  
   1.8 Ongoing Explanatory Work .................................... 11  

2 **Achieving Anti-fragility** .................................. 13  
   2.1 Black and Gray Swans .......................................... 13  
   2.2 Examples of Swans ............................................. 15  
   2.3 Limiting the Impact of Failures ............................... 16  
   2.4 Learning from Small Failures ................................ 17  
   2.5 An Alternative Justification ................................ 18  
   2.6 Risk Analyses Ignore Swans .................................. 19  
   2.7 Understanding and Reducing Risk ............................. 20  
   2.8 Taleb’s Four Quadrants ....................................... 21  
   2.9 Discussion and Summary ..................................... 22  

3 **The Need to Build Trust** .................................. 25  
   3.1 Defining Trust ................................................ 25  
   3.2 Explanatory Trust Model ....................................... 27  
   3.3 Model Limitations ............................................. 29  
   3.4 Trust Is Fragile ............................................... 29  
   3.5 Distrust Is Robust ............................................. 31
3.6 Maintaining Trust

3.6.1 Prepare Alternative Services

3.6.2 Make Digital Services Voluntary

3.6.3 Build a Good Track Record

3.7 Discussion and Summary

4 Principles Ensuring Anti-fragility

4.1 Modularity

4.2 Weak Links

4.3 Redundancy

4.4 Diversity

4.5 Fail Fast

4.6 Systemic Failure Without Failed Modules

4.7 The Need for Models

4.8 Discussion

Part II Anti-fragility to Downtime

5 Anti-fragile Cloud Solutions

5.1 Choice of System Realization

5.2 Modularity via Microservices

5.3 Weak Links via Circuit Breakers

5.4 Redundancy Provided by the Cloud

5.5 Diversity Enabled by the Cloud

5.6 Fail Fast Using Software Tools

5.7 Top–Down Design and Bottom–Up Tinkering

5.8 Discussion and Summary

6 Toward an Anti-fragile e-Government System

6.1 The Norwegian e-Government System

6.2 Redesign Needed

6.3 Better Testing

6.4 Availability Requirements

6.5 Fine-Grained SOA in a Public Cloud

6.6 User-Focused and Iterative Development

6.7 Single Versus Multiple Systems

6.7.1 Systems with Strongly Connected Modules

6.7.2 Cloud-Based Systems of Weakly Connected Modules

6.8 Discussion and Summary

7 Anti-fragile Cloud-Based Telecom Systems

7.1 Anti-principles Causing Fragility to Downtime

7.2 Past Fragility to Downtime

7.3 Indicators of Fragility to Future Downtime

7.4 Robust Access Networks
7.5 Robust Network Core ........................................ 75
7.6 Reduced Dependency on the Power Grid .................. 75
7.7 Reduced Dependency on One Infrastructure ............... 76
7.8 Anti-fragility to Downtime .................................. 76
7.9 Discussion and Summary .................................... 77

Part III  Anti-fragility to Malware

8 Robustness to Malware Spreading ............................ 81
  8.1 Introduction .................................................. 81
  8.2 Explanatory Epidemiological Model ....................... 82
     8.2.1 Epidemiological Model ............................... 82
     8.2.2 Non-predictive Model ............................... 83
  8.3 Malware-Halting Technique ............................... 84
  8.4 Halting Technique Analysis ............................... 85
  8.5 Halting Technique Performance ......................... 87
     8.5.1 Sparse and Homogeneous Networks .................. 87
     8.5.2 Dense and Homogeneous Networks .................. 89
  8.6 Persistent Targeted Attacks .............................. 89
  8.7 Related Work ............................................... 90
  8.8 Summary .................................................... 92

9 Robustness to Malware Reinfections ....................... 93
  9.1 Malware Attack on a Norwegian Bank .................... 93
  9.2 Stochastic Epidemiological Model ....................... 94
  9.3 How to Immunize Unknown Hubs ......................... 95
  9.4 Lower Bound on Required Diversity ..................... 96
  9.5 Discussion and Summary ................................ 97

10 Anti-fragility to Malware Spreading ....................... 99
  10.1 System Model .............................................. 100
     10.1.1 Model Description .................................. 101
     10.1.2 Model Limitations .................................. 102
  10.2 Anti-fragility on Static Graphs ......................... 103
     10.2.1 Simulations of Anti-fragility on Static Networks . 104
     10.2.2 Anti-fragility on Large Static Networks .......... 105
  10.3 Anti-fragility on Time-Varying Graphs .................. 105
     10.3.1 Simulations of Anti-fragility ...................... 106
  10.4 Discussion ................................................ 109

Part IV  Anomaly Detection

11 The HTM Learning Algorithm ................................. 113
  11.1 The Problem with Classical AI Research ............... 114
  11.2 An Alternative Approach to Learning .................. 114