Digital Asset Valuation and Cyber Risk Measurement
Principles of Cybernomics

Keyun Ruan
1. Digital Assets as Economic Goods

1.1 Origins and Philosophical Concepts of Value
   1.1.1 Subjective View Versus Objective View
   1.1.2 Intrinsic Value Versus Extrinsic Value

1.2 What Is an Economic Good?
1.3 What Is an Asset?
   1.3.1 Definition of Asset
   1.3.2 Current Asset Valuation Methods

1.4 What Are Digital Assets?
   1.4.1 Categorization of Digital Assets
      1.4.1.1 (Networked) System Assets
      1.4.1.2 Software Assets
      1.4.1.3 Hardware Assets
      1.4.1.4 Service Assets
      1.4.1.5 Robotic Assets
      1.4.1.6 Data Assets
      1.4.1.7 Metadata Assets
      1.4.1.8 Digitally Enabled Devices
   1.4.2 Managing Digital Assets in an Organization
      1.4.2.1 Information Resource Management
      1.4.2.2 Digital Assets Management

1.5 Unique Attributes of Digital Assets
   1.5.1 Characteristic 1: Digital Value Creation Does Not Decrease but Increases Through Usage
   1.5.2 Characteristic 2: Duplication Does Not Increase Digital Value
   1.5.3 Characteristic 3: Digital Value Production and Distribution Entails Higher Fixed Costs and Lower Variable Costs
   1.5.4 Characteristic 4: Digital Value Can Be Distributed via Multi-Sided Markets

1.6 Digital Value Matrix: Categorization of Digital Assets Based on Their Economic Functions
   1.6.1 Digital Asset on an Individual Level
   1.6.2 Digital Asset on an Organizational Level
   1.6.3 Digital Asset on a National Level
   1.6.4 Digital Asset on the Global Level

1.7 Valuation of Digital Assets as Economic Goods
   1.7.1 Attributes of Digital Assets Contribute to Intrinsic Digital Value Creation
      1.7.1.1 Data Quality
      1.7.1.2 Risk Exposure
      1.7.1.3 Age
      1.7.1.4 Data Volume
      1.7.1.5 System Quality
      1.7.1.6 Production Cost
   1.7.2 Attributes of Digital Assets Contribute to Extrinsic Digital Value Creation
      1.7.2.1 Exclusivity
      1.7.2.2 Network Connectivity
      1.7.2.3 Accessibility
      1.7.2.4 Reproduction Cost
      1.7.2.5 Economies of Scale
      1.7.2.6 Data Format
      1.7.2.7 Level of Structure
      1.7.2.8 Delivery Cadence
      1.7.2.9 Power Supplies

1.8 Existing Challenges for Digital Asset Valuation
   1.8.1 Inherent Challenges
   1.8.2 Market Challenges
2.4.4 Law of Subjectivity 45

2.4.4.1 Phenomenon 4a: The Need to Be Entertained 45

2.4.4.2 Phenomenon 4b: The Demand for Customization 46

2.4.4.3 Principle 4: A Greater Component of Value Is Increasingly Subjective, Reflecting Only in an Entity's Willingness-to-Pay 46

2.4.5 Law of Abundance 46

2.4.5.1 Phenomenon 5: Once Intrinsic Digital Value is Created, There are Limitless Ways to Multiply it with Extrinsic Digital Value 46

2.4.5.2 Principle 5a: The Digitally Empowered Entity has Limitless Economic Potential 46

2.4.5.3 Principle 5b: Consumer Reception and Power Supply Are Limiting Factors 46

2.4.5.4 Principle 5c: The Attention of a Consumer Is the New Scarce Resource 46

2.4.6 Law of New Division of Labor 47

2.4.6.1 Phenomenon 6a: Labor Is Increasingly a Less Important Factor in Value Production 47

2.4.6.2 Phenomenon 6b: New Necessities and the Barrier to Entry in a Digitized Society 47

2.4.6.3 Phenomenon 6c: Deep Learning and Machine Intelligence Are Still Inherently Limited 47

2.4.6.4 Phenomenon 6d: Accuracy Is Not the Truth 48

2.4.6.5 Principle 6a: The Digital Economy Is Creating a New Social Divide Based on the New Labor Value Chain 48

2.4.6.6 Principle 6b: The Optimal Path to Intrinsic Value Creation Is a Combination of Human and Machine Intelligence 48

3. Cyber Risk Management: A New Era of Enterprise Risk Management 49

3.1 History and Definitions of Risk 49

3.1.1 History of Risk 49

3.1.2 Definitions of Risk as a Multidimensional Concept 50

3.1.3 Risk in Computer Science and Engineering 50

3.1.4 Risk Can Only Be Relatively Objective 51

3.1.5 Decision Theory and Acceptable Risk 51

3.2 Enterprise Risk Management 52

3.2.1 The Discipline of Enterprise Risk Management 52

3.2.2 Cyber Risk Management: A New Era of Enterprise Risk Management 53

3.3 Risk Analysis 55

3.4 Risk Management 57

3.4.1 Risk Assessment 57

3.4.1.1 Define the Risk Assessment Process 57

3.4.1.2 System Characterization 57

3.4.1.3 Risk Classification 57

3.4.1.4 Threat Identification 57

3.4.1.5 Vulnerability Assessment 63

3.4.1.6 Likelihood Determination 66

3.4.1.7 Impact Analysis 67

3.4.1.8 Risk Determination 67

3.4.2 Risk Mitigation 68

3.4.3 Effectiveness Assessment 70

3.4.4 Continuous Monitoring 70

3.5 Risk Models 70

3.5.1 Qualitative and Quantitative Models 70

3.5.2 Quantitative Assessment 70

3.5.3 Qualitative Assessment 71

3.5.4 Other Models 71

3.5.4.1 Perspective: Asset-driven, Service-driven, or Business driven 72

3.5.4.2 Resource Valuation: Vertical or Horizontal 72

3.5.4.3 Risk Measurement: Propagated or Nonpropagated 72

4. Cyber Risk Measurement in the Hyperconnected World 75

4.1 Cyber Risk as a Critical Business Risk 75

4.2 The Uniqueness of Cyber Risk 76

4.3 The Need for Cyber Risk Measurement and Current Challenges 77

4.4 Cost Models for Incidents and Losses 78

4.4.1 Cost of Cybercrime 78

4.4.2 Cyber incident loss Categories 79

4.4.3 Models for Measuring Expected Loss 79

4.4.3.1 Expected Loss 79

4.4.3.2 Expected Severe Loss 79

4.4.3.3 Standard Deviation of Loss 79

4.4.3.4 Perceived Composite Risk 80

4.4.3.5 Loss in Market Value 82
4.5 Methods for Cyber Risk Measurement 82
4.5.1 Stochastic Modeling 82
4.5.2 Monte Carlo Simulation 83
4.5.3 Cyber Value at Risk 83
4.5.4 The CORAS Method 83
4.5.5 Common Vulnerability Scoring System 83
4.5.6 Factor Analysis of Information Risk 84

4.6 Introducing Cyber Risk Quadrant: Applying Medical Risk Measurement to Cyber 84
4.6.1 Applying Medical Risk Model for Measuring Cyber Risk 84
4.6.2 Using Scenario Analysis for Control Assessment and Loss Quantification 85

5. Economic Modeling and the Implementation of Effective Mitigating Controls 87
5.1 Definition of Control and Types of Controls 87
5.1.1 Definition of Control 87
5.1.2 Types of Control 88
  5.1.2.1 Control Objectives for Information and Related Technology 89
  5.1.2.2 NIST SP 800-53 90
  5.1.2.3 Committee of Sponsoring Organizations of the Tortway Commission 91
  5.1.2.4 ISO/IEC 27002 91
  5.1.2.5 Information Technology Infrastructure Library 91
5.1.3 Control Selection and Implementation 92
  5.1.3.1 CIS Critical Security Controls 92
  5.1.3.2 National Institute of Standards and Technologies Information Security Management System 93
5.2 Prioritizing Cost-Effective Controls 93
5.3 Measuring Cost of Controls 94
  5.3.1 The Balance Sheet-Oriented Approach 94
  5.3.2 The Security Measure Life-Cycle Approach 94
  5.3.3 IT Security Process-Oriented Approach 95
  5.3.4 Cost to Break 95
5.4 Measuring Benefits of Controls 95
  5.4.1 Security Performance Metrics 96
  5.4.2 Vulnerability Assessments 97
  5.4.3 Penetration Testing 97
  5.4.4 Internal Audit 97

6. The Point of Diminishing Return on Cyber Risk Investment 99
6.1 Economics of Information Security 99
6.2 Current Information Security/Risk Management Budget 102
6.3 Challenges for Cyber Risk Management Cost Optimization 104
  6.3.1 The Challenges in Quantifying Security Costs 104
    6.3.1.1 Cyber Security and Risk Management Is a Cross-Functional Task 104
    6.3.1.2 Divergent Goals Exist for Cost Quantification 104
    6.3.1.3 Lack of Transparency on Hidden Costs 104
    6.3.1.4 Difficulties in Finding the Right Scope and Baseline 105
    6.3.1.5 Lack of Resources and Clear Ownership to Implement Controls 105
  6.3.2 Challenges in Determining the Optimal Level of Investment in Security and Risk 105
  6.3.3 General Limitations of Approaches: Game Theory in Security Investment 106
6.4 Current Models for Cyber Risk Cost Optimization 106
  6.4.1 Cost Models for Determining how much to Investment in Security and Risk 106
    6.4.1.1 Benchmarking 106
    6.4.1.2 Cost-Benefit Analysis 107
    6.4.1.3 Quantitative Risk Assessment 107
    6.4.1.4 Return on Security Investment 107
    6.4.1.5 Net Present Value 108
    6.4.1.6 Internal Rate of Return 109
    6.4.1.7 Comparisons of Return on Investment, Net Present Value and Internal Rate of Return 109
    6.4.1.8 Gordon and Loeb Model 110
    6.4.1.9 Full Cost Accounting Model 111
  6.4.2 Cost Models for Projection 112
  6.4.3 Risk Management Options and Associated Cost 113
    6.4.3.1 Defense-in-Depth and Holistic Thinking 113
6.5 Cost of Security Configurations 113
6.6 Decision Model for Optimal Risk Management Strategies 115

7.1 Risk Metrology 117
7.1.1 History of Metrology 117
7.1.2 Traceability and Calibration 119
7.1.3 Uncertainty 119
7.1.4 Metrology and Cyber Risk 120

7.2 Micromort 120
7.2.1 Willingness-to-Pay and Value of a Micromort 120
7.2.2 Value of a Statistical Life 121
7.2.3 Microlife 121

7.3 Value-at-Risk 122

7.4 Introducing Bitmort and Hekla 123

7.5 Risk Calculations 125
7.5.1 Measuring Strength of Controls for Digital Assets Using Bitmort 125
7.5.2 Measuring Cost-Effectiveness of Controls for Digital Assets Using Bitmort 125
7.5.3 Articulating an Entity’s “Willingness-to-Pay” for Risk Reduction for Digital Assets Using Bitmort 125
7.5.4 Articulating an Entity’s Cyber Risk Limit Using Hekla 125
7.5.5 Articulating an Entity’s Cyber Risk Appetite Using Hekla 125
7.5.6 Measuring an Entity’s Cyber Risk Pricing Using Hekla 125
7.5.7 Measuring an Entity’s Cost of Risk Reduction Using Hekla 125
7.5.8 Measuring an Entity’s Cyber Risk Return on Investment Using Hekla 126
7.5.9 Using Bitmort and Hekla on a Portfolio of Entities 126

8. Three Views of Cybernomics: Entity View, Portfolio View, and Global View 127

8.1 Cybernomics 127
8.2 Portfolio Level 128
8.2.1 Supplier Risk 128
8.2.2 Systemic Risk 129
8.2.2.1 Systemic Cyber Risk in Financial Services Sector 129
8.2.2.2 Systemic Cyber Risk in Transportation Sector 130
8.2.2.3 Systemic Cyber Risks in the Healthcare Sector 131
8.2.3 National Digital Strategies and Policies 132

8.2.4 Cyber Regulations 132
8.2.4.1 General Data Protection Regulation 132
8.2.4.2 NIS Directive 133
8.2.4.3 Cybersecurity Act of 2015 133
8.2.4.4 FISMA Reform 133
8.2.4.5 Gramm–Leach–Bliley Act 134
8.2.4.6 Health Insurance Portability and Accountability Act 134

8.3 Global Level 134
8.3.1 Major Infrastructural Cyber Threats 134
8.3.1.1 Major Worms 134
8.3.1.2 Cyber Terrorism 136
8.3.1.3 Mega Data Breaches 136
8.3.1.4 Privacy Concerns of Technology Giants 137
8.3.2 Risk Data Schemes and Data Sharing: Barriers and Solutions 137
8.3.3 Cyber Infrastructure as a Public Good and the Privatization of the Internet 138

8.4 Three Views of Cybernomics 138
8.4.1 Entity Level 138
8.4.2 Portfolio Level 139
8.4.3 Global Level 140

9. Principles of Cybernomics 141

9.1 Unique Attributes of Digital Assets 142
9.1.1 Characteristic 1: Digital Value Creation Does Not Decrease, but Increases, Through Usage 142
9.1.2 Characteristic 2: Duplication Does Not Increase Digital Value 142
9.1.3 Characteristic 3: Digital Value Production and Distribution Entails Higher Fixed Costs and Lower Variable Costs 142
9.1.4 Characteristic 4: Digital Value Can Be Distributed Via Multi-Sided Markets 143
9.1.5 Characteristic 5: Digital Value Is Limitless 143
9.1.5.1 Characteristic 5a: Digital Value Has Limitless Utility to the Owner 143
9.1.5.2 Characteristic 5b: There Are Limitless Opportunities to Distribute and Consume Digital Value 144

9.2 Digital Value Matrix: Categorization of Digital Assets Based on Their Economic Functions 144

9.3 Characteristics of the Fourth Industrial Revolution 145
9.3.1 Characteristic 1: Velocity 145
9.3.2 Characteristic 2: Cross-Jurisdictional Economies of Scale Without Mass 145
9.3.3 Characteristic 3: Heavy Reliance on Intangible Assets, Especially Intellectual Property 145
9.3.4 Characteristic 4: The Importance of Data, User Participation, and Their Synergies With Intellectual Property 145
9.3.5 Characteristic 5: Fusion of Technologies 146
9.3.6 Characteristic 6: Consumption Externalities 146
9.3.7 Characteristic 7: Indirect Network Effects 146
9.3.8 Characteristic 8: Lock-In Effects and Competition 146
9.4 Models for Digital Asset Valuation 146
9.4.1 Method 1: Intrinsic Value 146
9.4.1.1 1a: Intrinsic Cost of Production 147
9.4.1.2 1b: Direct Financial Conversion 147
9.4.2 Method 2: Extrinsic Value 147
9.4.2.1 2a: Market Value 147
9.4.2.2 2b: Usage Value 147
9.4.3 Method 3: Subjective Value 147
9.4.4 Method 4: Opportunity Value 147
9.5 Measuring the Digital Economy 148
9.6 Digital Theory of Value 148
9.6.1 Law of Machine Time 149
9.6.1.1 Principle 1a: Progress of Digital Economy Should Be Measured Against Machine Time 149
9.6.1.2 Principle 1b: Sensemaking Is a Universal Challenge and a Value Driver 149
9.6.1.3 Principle 1c: Risk Management Is an Island of Stability in the Sea of Change 149
9.6.2 Law of Recombination 149
9.6.2.1 Principle 2: Recombination Is an Engine for Growth 149
9.6.3 Law of Hyperconnectivity 150
9.6.3.1 Principle 3a: Hyperconnectivity Is an Engine for Growth 150
9.6.3.2 Principle 3b: The Gravity of Value Creation will be Increasingly in the Virtual Space Where Value Creation Is Location Independent 150
9.6.3.3 Principle 3c: Nontechnical Barriers, Such As Geopolitical, Regulations, Legal Frameworks, Are Limiting Factors 150
9.6.4 Law of Subjectivity 150
9.6.4.1 Principle 4: A Greater Component of Value Is Increasingly Subjective, Reflecting Only in an Entity’s Willingness-to-Pay 150
9.6.5 Law of Abundance 150
9.6.5.1 Principle 5a: The Digitally Empowered Entity has Limitless Economic Potential 150
9.6.5.2 Principle 5b: Consumer Reception and Power Supply are Limiting Factors 150
9.6.5.3 Principle 5c: The Attention of a Consumer Is the New Scarce Resource 151
9.6.6 Law of the New Division of Labor 151
9.6.6.1 Principle 6a: The Digital Economy Is Creating a New Social Divide Based on the New Labor Value Chain 151
9.6.6.2 Principle 6b: The Optimal Path to Intrinsic Value Creation Is a Combination of Human and Machine Intelligence 151
9.7 Cyber Risk Quadrant: Applying Medical Risk Measurement to Cyber 151
9.7.1 Applying Medical Risk Model for Measuring Cyber Risk 151
9.7.2 Using Scenario Analysis for Control Assessment and Loss Quantification 152
9.8 Introducing Bitmort and Hekla 153
9.9 Risk Calculations 155
9.9.1 Measuring Strength of Controls for Digital Assets Using Bitmort 155
9.9.2 Measuring Cost-Effectiveness of Controls for Digital Assets Using Bitmort 155
9.9.3 Articulating an Entity’s “Willingness-to-Pay” for Risk Reduction for Digital Assets Using Bitmort 155
9.9.4 Articulating an Entity’s Cyber Risk Limit Using Hekla 155
9.9.5 Articulating an Entity’s Cyber Risk Appetite Using Hekla 155
9.9.6 Measuring an Entity’s Cyber Risk Pricing Using Hekla 155
9.9.7 Measuring an Entity's Cost of Risk Reduction Using Hekla 155
9.9.8 Measuring an Entity's Cyber Risk Return on Investment Using Hekla 156
9.9.9 Using Bitmort and Hekla on a Portfolio of Entities 156

9.10 Three Views of Cybernomics 156
9.10.1 Entity View 157
9.10.2 Portfolio View 157
9.10.3 Global View 157

9.11 Discussions and Limitations 157
9.11.1 Accuracy 157
9.11.2 Analytical Capabilities 158
9.11.3 Testing and Validation 158
9.11.4 Economic Lifespan of Digital Assets 158
9.11.5 Fundamental Inherent Differences of Digital Assets 158

10. Case Study: Insuring the Future of Everything 159
10.1 History and Context of Cyber Insurance 159
10.2 Current Offerings, Coverage, and Policy Limits 161

10.2.1 Current Policy Coverage 161
10.2.2 Types of Breaches That Lead to Claims 162
10.2.3 Reputation Loss as Part of First-Party Loss 163
10.2.4 Policy Limits 163

10.3 Underwriting and Assessment Process 164
10.3.1 Conducting a Thorough Information Security Risk Audit 164
10.3.2 Assessing Current Coverage 164
10.3.3 Evaluating Available Policies 164
10.3.4 Selecting Appropriate Policies 164

10.4 Claim Study 165
10.5 Current Challenges in the Cyber Insurance Market 165
10.5.1 Lack of Sufficient Quality Actuarial Data 166
10.5.2 Asymmetric Information 167

10.6 Cybernomics and the Future Growth of the Cyber Insurance Market 167

References 169
Index 179