

Table of Contents

CHAPTER ONE. INTRODUCTION..... 1

1.1 OVERVIEW 1

 1.1[a] *Brief History of Computing in the Cybersecurity Context*..... 1

 1.1[b] *Introduction to the Relationship Between Cybersecurity, Cybersecurity Law and Privacy Law and “Reasonable Security Measures”*. 4

1.2 WHAT IS CYBERSECURITY LAW? 6

1.3 RESPONSIBILITIES OF A CYBERSECURITY PROFESSIONAL..... 9

 1.3[a] *Vulnerability Analysis*..... 9

 1.3[b] *Cybersecurity Tools* 15

 1.3[c] *Inhouse Development of Products and Services* 21

 1.3[d] *Incident Response Responsibilities*..... 23

1.4 RESPONSIBILITIES OF A CYBERSECURITY COUNSELOR 24

CHAPTER TWO. FEDERAL TRADE COMMISSION ENFORCEMENT AND CYBERSECURITY LAW 27

2.1 INTRODUCTION..... 27

2.2 WYNDHAM AND SUBSEQUENT ENFORCEMENT ACTIONS 29

2.3 THE SUFFICIENCY OF FTC COMPLAINTS: D-LINK SYSTEMS..... 34

2.4 THE LABMD MATTER 36

CHAPTER THREE. THE GRAMM-LEACH-BLILEY ACT AND FTC SAFEGUARDS RULE 38

3.1 INTRODUCTION..... 38

3.2 FTC’S JURISDICTION UNDER GLBA..... 38

3.3 GLBA AND FTC SAFEGUARDS RULE 39

3.4 FTC GBLA/FTC SAFEGUARDS RULE CASES 40

3.5 PRIVATE CAUSE OF ACTION USING GLBA AND SAFEGUARDS RULE 42

3.6 OTHER LEGAL REGULATION CONCERNING FINANCIAL INSTITUTIONS..... 44

 3.6[a] *Security Guidelines*..... 47

 3.6[b] *Enforcement*..... 49

 3.6[b][i] OCC Enforcement 49

 3.6[b][ii] FDIC Enforcement 51

 3.6[c] *National Credit Union Administration* 53

 3.6[d] *U.S. Commodity Futures Trading Commission* 56

 3.6[e] *Federal Financial Institutions Examination Council*..... 57

CHAPTER FOUR. U.S. SECURITIES AND EXCHANGE COMMISSION CYBERSECURITY 60

4.1 INTRODUCTION..... 60

4.2 REGULATION S-P AND REGULATION SCI..... 60

4.3 SEC ENFORCEMENT 64

4.3[a] Overview of SEC Enforcement Actions	65
4.3[b] SEC Enforcement Actions	65
4.4 PRIVATE LITIGATION CONCERNING SECURITIES FRAUD FOR DATA BREACH	68
4.5 SEC ORDER FOR FAILURE TO DISCLOSE BREACH UNDER SECURITIES REPORTING LAWS	70
CHAPTER FIVE. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	71
5.1 INTRODUCTION.....	71
5.2 THE HIPAA SECURITY RULE AND BREACH NOTIFICATION RULES	71
5.3 OFFICE OF CIVIL RIGHTS ENFORCEMENT ACTIONS CONCERNING HIPAA.....	85
5.4 PRIVATE LITIGATION AND HIPAA.....	90
CHAPTER SIX. FAMILY EDUCATION RIGHTS AND PRIVACY ACT	93
6.1 INTRODUCTION.....	93
6.2 FERPA.....	93
6.2[a] DOE Guidance from the Privacy Technical Assistance Center.....	96
6.2[b] Additional Cybersecurity Requirements for Title IV Schools.....	97
6.2[c] Office of Inspector General U.S. Department of Education Technology Crimes Division.....	100
CHAPTER SEVEN. STATE CYBERSECURITY LAWS.....	103
7.1 INTRODUCTION.....	103
7.2 STATE BREACH NOTIFICATION LAWS.....	103
7.2[a] National Conference of State Legislatures on Security Breach Notification Laws.....	104
7.2[b] Example Private Cause of Actions Cases Brought Under State Breach Notification Laws.....	105
7.3 DATA SECURITY LAWS.....	108
7.3[a] Specific Data Security Laws.....	108
CHAPTER EIGHT. ADDITIONAL PRIVATE CAUSES OF ACTION FOR CYBERSECURITY BREACHES	115
8.1 INTRODUCTION.....	115
8.2 STANDING	115
8.3 OTHER COMMON LAW AND STATUTORY CAUSES OF ACTION.....	118
8.4 CLASS CERTIFICATION	123
CHAPTER NINE. CYBERSECURITY RISK ASSESSMENT AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RISK MANAGEMENT FRAMEWORK.....	128
9.1 INTRODUCTION.....	128
9.2 RISK ASSESSMENT	128
9.2[a] Risk Analysis.....	128

9.3 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RISK MANAGEMENT FRAMEWORK	133
9.3[a] <i>Overview of the NIST Risk Management Framework</i>	133
9.4 THE NIST RISK MANAGEMENT FRAMEWORK: SELECTED INFORMATION	137
9.4[a] <i>NIST 800 Series of Special Publications</i>	138
9.4[a][i] Federal Information Processing Standards, NIST Special Publications and NIST Interagency Reports	142
CHAPTER TEN. LAWS PROHIBITING AND ADDRESSING HACKING	168
10.1 INTRODUCTION.....	168
10.2 FEDERAL COMPUTER FRAUD AND ABUSE ACT.....	168
10.2[a] <i>Unauthorized Access or Access Exceeding Authorization</i>	172
10.2[b] <i>Damage or Loss</i>	174
10.3 STATE ANTI-HACKING LAWS: WASHINGTON AND CALIFORNIA	175
10.3[a] <i>Washington State Law</i>	175
10.3[b] <i>California State Law</i>	179
10.4 DEFEND TRADE SECRETS ACT AND ECONOMIC ESPIONAGE ACT.....	186
10.4[a] <i>Defend Trade Secrets Act</i>	186
10.4[b] <i>Economic Espionage Act</i>	190
10.5 STORED COMMUNICATIONS ACT.....	193
10.5[a] <i>Selected Provisions of the Stored Communications Act and Discussion</i>	194
10.6 DIGITAL MILLENNIUM COPYRIGHT ACT	197
10.6[a] <i>Selected Provisions of the Digital Millennium Copyright Act</i>	197
10.6[b] <i>DMCA Cases</i>	200
CHAPTER ELEVEN. INTERNET OF THINGS	205
11.1 INTRODUCTION.....	205
11.2 IOT BACKGROUND INFORMATION	205
11.3 NIST GUIDANCE DOCUMENT: FOUNDATIONAL CYBERSECURITY ACTIVITIES FOR IOT DEVICE MANUFACTURERS	211
11.4 CALIFORNIA’S INTERNET OF THINGS LEGISLATION	211
11.5 COMPLAINT CONCERNING INTERNET OF THINGS AND CYBERSECURITY	214
11.6 NIST SPECIAL PUBLICATION 1800-15 SECURING SMALL-BUSINESS AND HOME INTERNET OF THINGS (IoT) DEVICES: MITIGATING NETWORK-BASED ATTACKS USING MANUFACTURER USAGE DESCRIPTION (MUD)	215
CHAPTER TWELVE. AN INTERNATIONAL PERSPECTIVE	217
12.1 INTRODUCTION.....	217
12.2 GDPR	217
12.3 EUROPEAN CONVENTION ON CYBERCRIME.....	220
12.4 TALLINN MANUAL.....	222
12.5 U.S. CYBERSPACE SOLARIUM COMMISSION REPORT.....	223
12.6 OVERVIEW OF TRADE AND CYBERSECURITY	226

12.7 ASIA-PACIFIC ECONOMIC COOPERATION CROSS-BORDER PRIVACY RULES SYSTEM 227

12.8 COMPREHENSIVE AND PROGRESSIVE AGREEMENT FOR TRANS-PACIFIC PARTNERSHIP
..... 228

12.9 UNITED STATES-MEXICO-CANADA AGREEMENT (ARTICLE 19 ET SEQ.) 231

12.10 THE FUTURE OF A MULTI-LATERAL COMPREHENSIVE TREATY ON CYBERSECURITY 233

INDEX 235