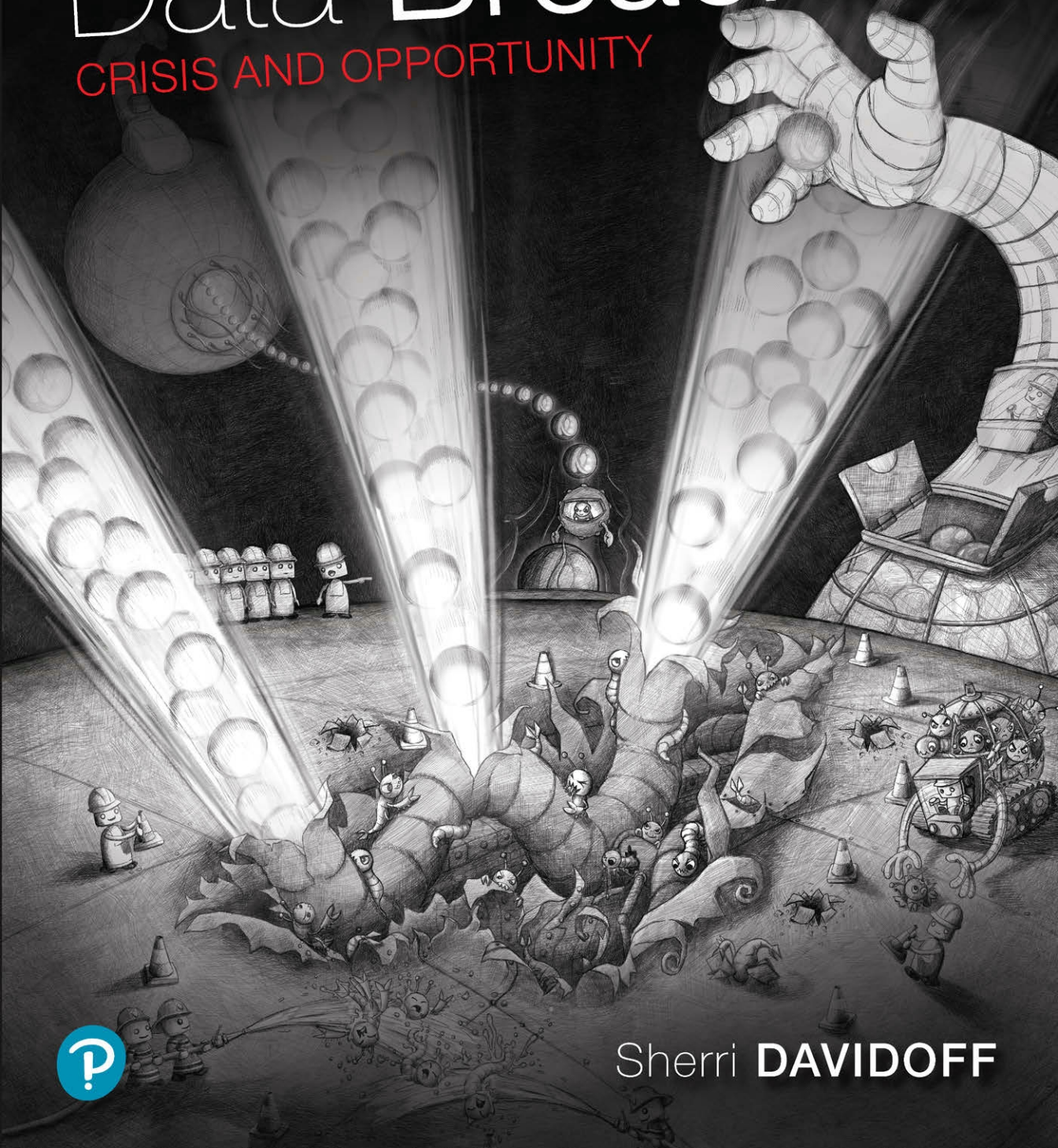




# Data Breaches

CRISIS AND OPPORTUNITY



Sherri **DAVIDOFF**

# *Data Breaches*

# **Data Breaches: Crisis and Opportunity**

## **Table of Contents**

Cover

Title Page

Copyright Page

Contents

Preface

Acknowledgments

About the Author

Chapter 1 Dark Matters

1.1 Dark Breaches

1.1.1 What Is a Data Breach?

1.1.2 Unprotected Personal Information

1.1.3 Quantifying Dark Breaches

1.1.4 Undetected Breaches

1.1.5 Dark and Darker Breaches

1.2 Skewed Statistics

1.2.1 Public Records

1.2.2 Raise Your Hand if Youve Had a Data Breach

1.2.3 Cybersecurity Vendor Data

1.3 Why Report?

1.4 Whats Left Unsaid

Chapter 2 Hazardous Material

2.1 Data Is the New Oil

2.1.1 Secret Data Collection

# **Table of Contents**

2.1.2 The TRW Breach

2.2 The Five Data Breach Risk Factors

2.3 The Demand for Data

2.3.1 Media Outlets

2.3.2 Big Advertising

2.3.3 Big Data Analytics

2.3.4 Data Analytics Firms

2.3.5 Data Brokers

2.4 Anonymization and Renonymization

2.4.1 Anonymization Gone Wrong

2.4.2 Big Data Killed Anonymity

2.5 Follow the Data

2.5.1 Pharmacies: A Case Study

2.5.2 Data Skimming

2.5.3 Service Providers

2.5.4 Insurance

2.5.5 State Government

2.5.6 Cost/Benefit Analysis

2.6 Reducing Risk

2.6.1 Track Your Data

2.6.2 Minimize Your Data

2.7 Conclusion

## **Chapter 3 Crisis Management**

3.1 Crisis and Opportunity

3.1.1 Incidents

3.1.2 Data Breaches Are Different

3.1.3 Recognizing Crises

3.1.4 The Four Stages of a Crisis

3.2 Crisis Communications, or Communications Crisis?

# **Table of Contents**

- 3.2.1 Image Is Everything
- 3.2.2 Stakeholders
- 3.2.3 The 3 Cs of Trust
- 3.2.4 Image Repair Strategies
- 3.2.5 Notification
- 3.2.6 Ubers Skeleton in the Closet

## **3.3 Equifax**

- 3.3.1 Competence Concerns
- 3.3.2 Character Flaws
- 3.3.3 Uncaring
- 3.3.4 Impact
- 3.3.5 Crisis Communications Tips

## **3.4 Conclusion**

# **Chapter 4 Managing DRAMA**

## **4.1 The Birth of Data Breaches**

- 4.1.1 Data Breaches: A New Concept Emerges
- 4.1.2 The Power of a Name

## **4.2 A Smoldering Crisis**

- 4.2.1 The Identity Theft Scare
- 4.2.2 The Product Is . . . You
- 4.2.3 Valuable Snippets of Data
- 4.2.4 Knowledge-Based Authentication
- 4.2.5 Access Devices

## **4.3 Prodromal Phase**

- 4.3.1 The Smoldering Crisis Begins . . .
- 4.3.2 Isn't It Ironic?
- 4.3.3 A Suspicious Phone Call
- 4.3.4 Hiding in Plain Sight
- 4.3.5 Recognize

# **Table of Contents**

4.3.6 Escalate

4.3.7 Investigate

4.3.8 Scope

## **4.4 Acute Phase**

4.4.1 Aint Nobody Here But Us Chickens

4.4.2 Just California . . . Really

4.4.3 . . . Oh, and Maybe 110,000 Other People

4.4.4 The Explosion

4.4.5 The Blame Game

4.4.6 That New Credit Monitoring Thing

4.4.7 Act Now, While Goodwill Lasts

## **4.5 Reducing Harm**

4.5.1 Devalue the Data

4.5.2 Monitor and Respond

4.5.3 Implement Additional Access Controls

## **4.6 Chronic Phase**

4.6.1 Call in the Experts

4.6.2 A Time for Introspection

4.6.3 Testifying before Congress

## **4.7 Resolution Phase**

4.7.1 The New Normal

4.7.2 Growing Stronger

4.7.3 Changing the World

## **4.8 Before a Breach**

4.8.1 Cybersecurity Starts at the Top

4.8.2 The Myth of the Security Team

## **4.9 Conclusion**

## **Chapter 5 Stolen Data**

# **Table of Contents**

## **5.1 Leveraging Breached Data**

## **5.2 Fraud**

### **5.2.1 From Fraud to Data Breaches**

## **5.3 Sale**

### **5.3.1 Selling Stolen Data**

### **5.3.2 Asymmetric Cryptography**

### **5.3.3 Onion Routing**

### **5.3.4 Dark E-Commerce Sites**

### **5.3.5 Cryptocurrency**

### **5.3.6 Modern Dark Data Brokers**

## **5.4 The Goods**

### **5.4.1 Personally Identifiable Information**

### **5.4.2 Payment Card Numbers**

### **5.4.3 Data Laundering**

## **5.5 Conclusion**

## **Chapter 6 Payment Card Breaches**

## **6.1 The Greatest Payment Card Scam of All**

## **6.2 Impact of a Breach**

### **6.2.1 How Credit Card Payment Systems Work**

### **6.2.2 Consumers**

### **6.2.3 Poor Banks**

### **6.2.4 Poor Merchants**

### **6.2.5 Poor Payment Processors**

### **6.2.6 Not-So-Poor Card Brands**

### **6.2.7 Poor Consumers, After All**

## **6.3 Placing Blame**

### **6.3.1 Bulls-Eye on Merchants**

### **6.3.2 Fundamentally Flawed**

### **6.3.3 Security Standards Emerge**

# **Table of Contents**

## **6.4 Self-Regulation**

6.4.1 PCI Data Security Standard

6.4.2 A For-Profit Standard

6.4.3 The Man behind the Curtain

6.4.4 PCI Confusion

6.4.5 QSA Incentives

6.4.6 Fines

## **6.5 TJX Breach**

6.5.1 Operation Get Rich or Die Tryin

6.5.2 Point-of-Sale Vulnerabilities

6.5.3 Green Hat Enterprises

6.5.4 The New Poster Child

6.5.5 Whos Liable?

6.5.6 Struggles with Security

6.5.7 TJX Settlements

6.5.8 Data Breach Legislation 2.0

## **6.6 The Heartland Breach**

6.6.1 Heartland Gets Hacked

6.6.2 Retroactively Noncompliant

6.6.3 Settlements

6.6.4 Making Lemonade: Heartland Secure

## **6.7 PCI and Data Breach Investigations**

6.7.1 PCI Forensic Investigators

6.7.2 Attorney-Client Privilege

## **6.8 Conclusion**

## **Chapter 7 Retailgeddon**

### **7.1 Accident Analysis**

7.1.1 Pileup

7.1.2 Small Businesses Under Attack



# **Table of Contents**

7.1.3 Attacker Tools and Techniques

## **7.2 An Ounce of Prevention**

7.2.1 Two-Factor Authentication

7.2.2 Vulnerability Management

7.2.3 Segmentation

7.2.4 Account and Password Management

7.2.5 Encryption/Tokenization

## **7.3 Targets Response**

7.3.1 Realize

7.3.2 The Krebs Factor

7.3.3 Communications Crisis

7.3.4 Home Depot Did a Better Job

## **7.4 Ripple Effects**

7.4.1 Banks and Credit Unions

7.4.2 Widespread Card Fraud

7.4.3 To Reissue or Not to Reissue?

## **7.5 Chip and Scam**

7.5.1 Alternate Payment Solutions

7.5.2 Card Brands Push Back

7.5.3 Changing the Conversation

7.5.4 Preventing Data Breaches . . . Or Not

7.5.5 Who Owns the Chip?

7.5.6 Public Opinion

7.5.7 Worth It?

7.5.8 No Chip, Please Swipe

## **7.6 Legislation and Standards**

## **7.7 Conclusion**

## **Chapter 8 Supply Chain Risks**

# **Table of Contents**

## **8.1 Service Provider Access**

8.1.1 Data Storage

8.1.2 Remote Access

8.1.3 Physical Access

## **8.2 Technology Supply-Chain Risks**

8.2.1 Software Vulnerabilities

8.2.2 Hardware Risks

8.2.3 Hacking Technology Companies

8.2.4 Suppliers of Suppliers

## **8.3 Cyber Arsenals**

8.3.1 Weapons Turned

8.3.2 Calls for Disarmament

## **8.4 Conclusion**

# **Chapter 9 Health Data Breaches**

## **9.1 The Public vs. the Patient**

9.1.1 Gaps in Protection

9.1.2 Data Breach Perspectives

## **9.2 Bulls-Eye on Healthcare**

9.2.1 Data Smorgasbord

9.2.2 A Push for Liquidity

9.2.3 Retention

9.2.4 A Long Shelf Life

## **9.3 HIPAA: Momentous and Flawed**

9.3.1 Protecting Personal Health Data

9.3.2 HIPAA Had No Teeth

9.3.3 The Breach Notification Rule

9.3.4 Penalties

9.3.5 Impact on Business Associates

## **9.4 Escape from HIPAA**

# **Table of Contents**

9.4.1 Trading Breached Data

9.4.2 Mandated Information Sharing

9.4.3 Deidentification

9.4.4 Reidentification

9.4.5 Double Standards

9.4.6 Beyond Healthcare

## **9.5 Health Breach Epidemic**

9.5.1 More Breaches? Or More Reporting?

9.5.2 Complexity: The Enemy of Security

9.5.3 Third-Party Dependencies

9.5.4 The Disappearing Perimeter

## **9.6 After a Breach**

9.6.1 Whats the Harm?

9.6.2 Making Amends

9.6.3 Health Breach Lawsuits

9.6.4 Learning from Medical Errors

## **9.7 Conclusion**

# **Chapter 10 Exposure and Weaponization**

## **10.1 Exposure Breaches**

10.1.1 Motivation

10.1.2 Doxxing

10.1.3 Anonymous

10.1.4 WikiLeaks

10.1.5 Weaponization

## **10.2 Response**

10.2.1 Verify

10.2.2 Investigate

10.2.3 Data Removal

10.2.4 Public Relations

# **Table of Contents**

## **10.3 MegaLeaks**

- 10.3.1 Mannings Crime
- 10.3.2 Caught!
- 10.3.3 Cooperation: A New Model
- 10.3.4 Drowning in Data
- 10.3.5 Redaction
- 10.3.6 Data Products
- 10.3.7 Timed and Synchronized Releases
- 10.3.8 Takedown Attempts Backfire
- 10.3.9 Distribution
- 10.3.10 Punishment Backfires
- 10.3.11 Copycats
- 10.3.12 Consequences

## **10.4 Conclusion**

## **Chapter 11 Extortion**

### **11.1 Epidemic**

- 11.1.1 Definition
- 11.1.2 Maturation

### **11.2 Denial Extortion**

- 11.2.1 Ransomware
- 11.2.2 Encryption and Decryption
- 11.2.3 Payment
- 11.2.4 World Domination
- 11.2.5 Is Ransomware a Breach?
- 11.2.6 Response

### **11.3 Exposure Extortion**

- 11.3.1 Regulated Data Extortion
- 11.3.2 Sextortion
- 11.3.3 Intellectual Property

# **Table of Contents**

11.3.4 Response

## **11.4 Faux Extortion**

11.4.1 Case Study: NotPetya

11.4.2 Response

## **11.5 Conclusion**

## **Chapter 12 Cyber Insurance**

### **12.1 Growth of Cyber Insurance**

### **12.2 Industry Challenges**

### **12.3 Types of Coverage**

### **12.4 Commercial Off-the-Shelf Breach Response**

12.4.1 Assessing Breach Response Teams

12.4.2 Confidentiality Considerations

### **12.5 How to Pick the Right Cyber Insurance**

12.5.1 Involve the Right People

12.5.2 Inventory Your Sensitive Data

12.5.3 Conduct a Risk Assessment

12.5.4 Review Your Existing Coverage

12.5.5 Obtain Quotes

12.5.6 Review and Compare Quotes

12.5.7 Research the Insurer

12.5.8 Choose!

### **12.6 Leverage Your Cyber Insurance**

12.6.1 Develop

12.6.2 Realize

12.6.3 Act

12.6.4 Maintain

12.6.5 Adapt

### **12.7 Conclusion**

# **Table of Contents**

## **Chapter 13 Cloud Breaches**

### **13.1 Risks of the Cloud**

13.1.1 Security Flaws

13.1.2 Permission Errors

13.1.3 Lack of Control

13.1.4 Authentication Issues

### **13.2 Visibility**

13.2.1 Business Email Compromise (BEC)

13.2.2 Evidence Acquisition

13.2.3 Ethics

### **13.3 Intercepted**

13.3.1 The Beauty of End-to-End Encryption

13.3.2 The Ugly Side of End-to-End Encryption

13.3.3 Large-Scale Monitoring

13.3.4 Investment in Encryption

### **13.4 Conclusion**

## **Afterword**

## **Index**