

TABLE OF CONTENTS

About the Authors

Foreword

Acknowledgements

Chapter 1 Overview of Cybersecurity and the Courts

Daniel Garrie, Esq. and Judge Leo M. Gordon

- § 1.01 Introduction: Court Vulnerability to Cyber Breaches
- § 1.02 Conclusion

Chapter 2 Essential Commandments of Cybersecurity

Daniel Garrie, Esq., Judge Leo M. Gordon, and Tim Murphy

- § 2.01 Introduction
- § 2.02 Develop and Practice Strong Cyber Hygiene
- § 2.03 Know and Secure Vendors' Networks
- § 2.04 Identify and Protect the "Crown Jewels"
- § 2.05 Practice Your Incident Response Plan
- § 2.06 Create and Develop a Global Communications and Messaging Framework
- § 2.07 Test the Incident Response Plan and Update It Regularly
- § 2.08 Develop a Robust Cyber Threat Monitoring and Sharing Team
- § 2.09 Engage Privacy and Cybersecurity Expertise
- § 2.10 Maintain Government Relationships

Chapter 3 A Survey of Cyber Threats and Their Context

Daniel Garrie, Esq., Judge Leo M. Gordon, David Lawrence, Tim Murphy, and Harvey Rishikof

- § 3.01 Introduction
- § 3.02 The State of Our Digital Union: Necessary Context for Adopting a Risk-Based Approach
- § 3.03 The Threats Landscape for Courts and Court Systems

- § 3.04 The Range of Specific Threats
- § 3.05 Conclusion

Chapter 4 What It Takes to Frustrate the Hacker Knocking at Your Door

Daniel Garrie, Esq., Judge Leo M. Gordon, Greg Kelley, Richard Rushing, and Bill Spernow

- § 4.01 Do not Be the Low-Hanging Fruit
- § 4.02 Proper Password Management Is Essential to Security
- § 4.03 Firewalls: Regulating Who and What Can Access Your System
- § 4.04 Applying Patches: Keeping Your Software as Secure and Up-to-Date as Possible
- § 4.05 Perimeter Security Controls: What It Takes to Keep the Bad Guys Out
- § 4.06 Encryption
- § 4.07 Summary

Chapter 5 Cryptography

Daniel Garrie, Esq., Judge Leo M. Gordon, Rick Borden, and Jeff Stapleton

- § 5.01 Introduction
- § 5.02 Encryption
- § 5.03 Message Authentication
- § 5.04 Digital Signatures
- § 5.05 Key Management
- § 5.06 Other Crypto Considerations
- § 5.07 Conclusion
- Appendix 5-1 Chapter Glossary

Chapter 6 ISO Standards

Daniel Garrie, Esq. and Judge Leo M. Gordon

- § 6.01 Introduction
- § 6.02 ISO Standard 27001
- § 6.03 ISO Scope and Certification
- § 6.04 Conclusion

Chapter 7 Defending Against Threats Through Information Sharing

Daniel Garrie, Esq., Judge Leo M. Gordon, Diana Burley, Cindy Donaldson, and Bill Nelson

- § 7.01 Legal Services: A Big Target for Hackers
- § 7.02 Attacks Are Getting More Frequent and More Sophisticated

TABLE OF CONTENTS

- § 7.03 There Is Hope: Courts and Court Systems Should Prepare and Share
- § 7.04 The Legal Services Information Sharing and Analysis Organization

Chapter 8 How Courts Can Use the Cybersecurity Framework for Critical Infrastructure

Daniel Garrie, Esq. and Judge Leo M. Gordon

- § 8.01 Introduction
- § 8.02 Overview of the NIST Framework
- § 8.03 The Framework Core: Functions of a Successful Cybersecurity Program
- § 8.04 Assessing Cybersecurity Risk Management Practices Using the Framework Implementation Tiers

Chapter 9 Structure Your Court to Make It Hacker-Proof

Daniel Garrie, Esq., Judge Leo M. Gordon, Greg Kelley, and Bill Spernow

- § 9.01 Internal Network Controls
- § 9.02 Threat Management Versus Risk Management
- § 9.03 Staff—Finding the Right People and Services
- § 9.04 Summary

Index