CISO STORIES

INSIDE THE INTERVIEW

Excerpts that inspired episodes of
CISO Stories from the acclaimed book, CISO Compass.

PRESENTED BY

CYBERSECURITY COLLABORATIVE

cybereason

CRC Press
Taylor & Francis Group

CISO COMPASS

NAVIGATING CYBERSECURITY LEADERSHIP CHALLENGES WITH INSIGHTS FROM PIONEERS

STRATEGY STRUCTURE SYSTEMS STAFF SKILLS STYLE SHARED VALUES

"COMPREHENSIVE ROADMAP WITH OVER 75 TOP CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY LEADERS."

TODD FITZGERALD

FOREWORD BY DR. LARRY PONEMON

MARK BURNETTE: THE BENEFITS OF FOCUSING ON RISK VS. COMPLIANCE

Shareholder, LBMC Information Security

Security compliance obligations represent a true irony for many security leaders. On the one hand, compliance obligations may provide the impetus that compels an organization to support and fund certain cybersecurity initiatives, providing some validation to the efforts of the security leader. However, on the other hand, in many cases, the business leaders at an organization are so focused on the entity's compliance obligations that they assume that once compliance is achieved, security is sufficient. Good security leaders know that true security is about proper cybersecurity risk management, and a well-designed program that enables company leaders to make well-informed decisions about security risks is the ideal state. Security leaders also agree that being compliant with an applicable security regulation does not necessarily equate to proper cybersecurity risk management (or sufficient security posture!). The challenge, then, is for security leaders to shift the mindset of their organization away from tracking compliance against regulations and towards the practice of security risk management. This shift is not easy, because company executives and board members are constantly bombarded by reminders of applicable rules and legislation, so they will continue to ask about the entity's compliance posture. When discussing and presenting your organization's compliance with the relevant regulations, be sure to continually bring the conversation back to how effectively cybersecurity risks are being identified, managed, and reported. Avoid building your dashboards and reports based on compliance posture if possible. While you will likely have to address the topic, an effective response can be something like "We expect to be fully compliant with XYZ law by the end of this year. While that is encouraging progress that we should acknowledge, XYZ law only applies to certain types of data, and we have at least three other types of sensitive data in our organization that must also be protected. Our most recent risk assessment highlighted the following areas of high risk. The company's security program and our security budget have been allocated to address those items by XXX date." Continually reinforce the concept of cybersecurity risk management with company leaders. Use data from your risk assessments to educate your executive team and inform their decision-making. If you can help them learn to make risk-based decisions rather than compliance-based reactions, your job satisfaction will be much higher, and your security program will be much more effective.

CISO COMPASS

Navigating Cybersecurity Leadership Challenges with Insights from Pioneers

Congratulations! You have been selected as the first Chief Information Security Officer (CISO) for your company. Time to celebrate! But, wait — what should you do next? Or maybe you are an experienced CISO and wonder — what can I learn from other successful CISOs to be even more effective? Or, are you considering a move from a technical career path and deciding if this is the right direction for you?

A CISO once honored as Chicago's CISO of the Year, author, and top-rated speaker on security issues, Todd Fitzgerald provides a comprehensive roadmap and much needed navigation to build, lead, and sustain a cybersecurity program. Todd adds straight talk — insightful stories and lessons learned from over 75 award-winning CISOs, highly-respected security leaders, professional association leaders, and cybersecurity standard setters who have also fought the tough battle.

You own your continued success as a security leader. If you want a roadmap to build, lead, and sustain a program respected and supported by your board, management, organization, and peers, this book is for you.

Want to learn more? Please visit www.cisocompass.com

"As the compass used for hiking, this "compass" points to the "true North" for success as a CISO. Todd brings together guidance, wisdom and direction from highly successful and prominent CISOs and information security leaders to provide a navigational tool to become a successful CISO. This book should be foundational reading for any degree in Information Security and should be on the desk of any current or future Information Security leader.

— **Steve Katz** (Recognized as the First CISO), Executive Advisor, Deloitte

"*CISO COMPASS* is a thorough roadmap to succeeding in one of the most challenging and important professions today. Now more than ever IT security professionals need to understand how best to demonstrate to senior management that the cybersecurity program they have built is supportive of their companies' business goals and mission. It is a welcome addition to the IT security body of knowledge."

—**Dr Larry Ponemon**, Ponemon Institute

Todd Fitzgerald has twenty years practical senior information security leadership experience building and leading multiple Fortune 500/large company security programs across industries, such as serving as the global Chief Information Security Officer for Grant Thornton International, Ltd. and ManpowerGroup.Todd authored several thought leading information security leadership books including ground-breaking *CISO Leadership: Essential Principles for Success, Information Security Governance Simplified: From the Boardroom to the Keyboard*, *E-C Council CISO Body of Knowledge,* and contributed to *ISC2 CISSP Official Study Guide*, *COBIT 5 for Information Security, ISACA CSX Cybersecurity Fundamentals Certification*, and many others. Todd is also an award-winning CISO and top-rated, sought-after speaker dedicated to sharing cybersecurity leadership knowledge and practices.

CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

CRC Press titles are available as eBook editions in a range of digital formats

INFORMATION TECNOLOGY

ISBN: 978-1-4987-4044-9