CISO STORIES

INSIDE THE INTERVIEW

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

PRESENTED BY CYBERSECURITY COLLABORATIVE | WIZ

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

- To enable business success through secure infrastructure and trusted transactions.
- Driving business objectives securely.
- To enable successful business outcomes, profitably and growth through balanced risk management, risk-aware culture, and the enablement of innovation.
- Deliver a program and strategy to protect our assets, values, and clients and reduce risk.
- Proactively provide: secure environment, deliver solutions to the business on time, securely, culture, enable security solutions to build confidence in the operations of the business and with customers, trusted companion of the business.
- Protect and enable the business to securely deliver the corporate mission in a digital transformation context.

Imagine if the CISO brought together members of the organization from different departments to construct the vision and spent more than 15 minutes on the exercise how rich and succinct the vision statement could become. The vision statements in the example above had common themes of business success, trust, and a sense of partnership. Security is never the end goal, and conducting business is the only reason security exists.

JASON CLARK: BUILDING A SECURITY VISION AND STRATEGY

Chief Strategy Officer, Netskope

An information security vision is the end result of an overall information security strategy, and in order to successfully establish a vision, you need to marry the vision to your strategy. That means that from day one, you need to be looking anywhere from 5 to 10 years ahead. Start asking yourself questions like "Where is the strategy of my company?" "Where does my organization want to go?" "What is its end goal?" "What are the forces giving me pressure (positive and negative), and how strong are they?" and "Given all of these forces, what are the steps I need to take to get to my desired outcome?"

Many strategies (and the vision associated with them) often fail because they have not been effectively communicated. In security, this is both an art and a science. There is science involved with understanding risk and threat models, but figuring out how to apply those models to the broader business and communicate it widely is an art. By clearly communicating your strategy in a digestible, visual format, your stakeholders will better understand the strategy. This puts you in a better position to equip your leader [CIO (Chief Information Officer), CEO, or the board] who will get the relevant

stakeholders aligned and inspire the whole organization (whether the security team, the IT team, or the wider business) to execute against that strategy and realize your vision.

Finally, CISOs are almost always a change agent in an organization. You are either the first CISO, or you have been brought in to replace a CISO. Ask yourself questions like "What can I do differently and make an impact to build something sustainable?" and "How can I market myself to the organization?" Speak in the language of the business and demonstrate to the wider organization that you are helping solve business problems. This will show them that your job is tied to the wider organization, critical to making their jobs more productive, and most importantly never finished.

Step 3—Examine Internal and External Environment Constraints

Companies work within the context of a much larger environment and are subject to external circumstances beyond what is created by them. These include the regulatory environment, strategies of the competitors, being aware of the emerging threats, knowing the cost structures, and leveraging the external independent research that is available.

Regulatory

Each organization should understand the regulatory environment within which they participate. Is the organization a publicly traded company subject to the Sarbanes–Oxley rules? Are they transacting business involving European citizens and subject to the General Data Protection Regulation (GDPR)? Do they maintain Protected Health Information and subject to the Health Insurance Portability and Accountability Act (HIPAA)? Are they complying with each state's security incident notification laws and aware of the New York State's Cybersecurity Requirements for Financial Services Companies effective March 1, 2017? Are they processing credit cards and subject to the Payment Card Industry Data Security Standards? The regulatory environment will drive security rules that have been mandated for the specific public or private sector.

Competition

Most board of directors want to know how the security strategy and investment compares with the strategy of their competitors. The objective of many companies is to spend no more and no less than that of their competitors, unless security is seen to provide a competitive advantage that is worth the additional investment.

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