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

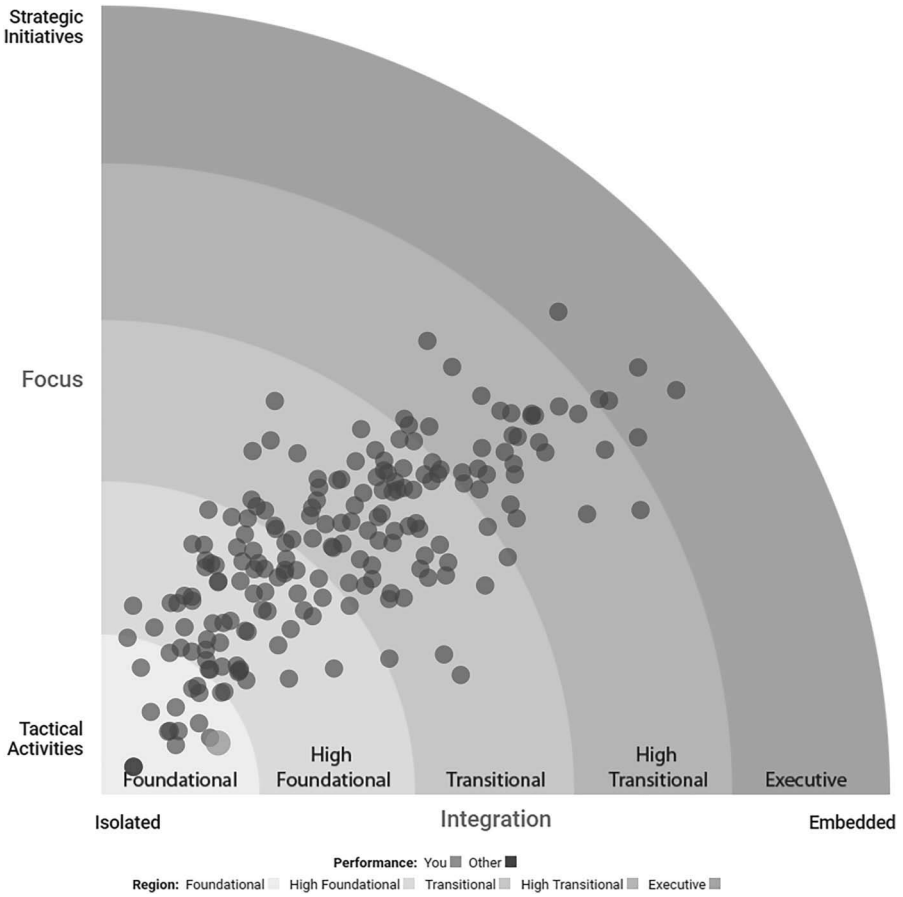

Figure 14.3 The CISO impact quotient. (From IANS, *CISO Impact: Lighting the Path to Leadership*, 2018. www.iansresearch.com/insights/reports/ciso-impact-lighting-the-path-to-leadership.)

DANE SANDERSEN: MOVING FROM A LARGE COMPANY TO SMALL- TO MEDIUM-SIZED COMPANY AS CISO

Global Security and Infrastructure Director, Trek Bicycle

So, you have decided to move on to a new, smaller company! Compared with a larger enterprise, you may notice a few differences—such as a less security savvy of the board of directors, lack of risk management allies, and you will probably be required to take a much more of a hands-on

approach. Whether you seek greater autonomy, or a better title, moving from a large enterprise to a small- to medium-sized business can be exciting and rewarding, but also can come with challenges too. The board of directors at a smaller company (if one exists at all) will likely not have the same understanding of security issues of their counterparts at a larger enterprise. You must start educating them gently and deliberately, covering both the low-hanging fruit and the big rocks that present the largest risks. Do not use FUD as a shortcut—you will likely lose their trust in the long term. One tactic to make quick progress with a security program is to "circle the wagons" with other risk managers. If they do not exist or are not up-to-date with the latest security information, you must work diligently to educate those that are present and root out others who are sensitive to protecting the company's information. I would also recommend seeking out senior leaders in the product, and financial departments, as they can be fantastic security advocates. Budgets and resources at smaller companies can seem meager compared with those at their larger counterparts. In many cases, you have to be willing to roll up your sleeves, wear multiple hats, and be able to react to a swiftly changing business environment. You also might not be able to hire the people you need or buy a platform you want. However, you might be able to borrow an IT resource to tighten down that department's controls, or piggyback a security initiative on an existing project. For many, the lure of a smaller business can be strong—you will be closer to the business, able to make a more of a difference, and have less rules to deal with… But, you will likely have an equal amount of challenges and may be in for a bit of culture shock. My advice is to be flexible, engaged, and stay motivated!

Soft Skills Are Hard and Require Practice

Soft skills involve understanding and interacting with people from different experiences, backgrounds, and their own motivations and current life situations. People are unpredictable and have their own "vulnerabilities." Practicing the soft skills increases the CISO's effectiveness to deliver on the technical aspects of the role. When the CISO was buried deep in the data center, it was possible to get by primarily on technical knowledge. This model has clearly changed, with the CISO operating at all levels of the organization, to be trusted and viewed as a business partner; these skills must be viewed as just as important, if not more, than the technical cybersecurity skills that advanced the technical security practitioner into the CISO role.

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