BUILD A SECURITY CULTURE

Kai Roer

Information Security buzz

itgp™

Build a Security Culture

Kai Roer

Build a Security Culture

KAI ROER

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing

ISBN 978-1-84928-717-3

ACKNOWLEDGEMENTS

This book is the direct result of my engagement and development of the Security Culture Framework. All the people who have been involved in the development and use of the framework are my inspiration to write this book.

The Security Culture Framework is something that evolved in my mind after many years of watching security awareness training programmes being run seemingly without control, metrics and proper planning. Discussing the topic with Lars Haug, we quickly came up with the concept of a holistic framework to help build and maintain security culture. The framework gained interest in both the USA and Europe, within both the public and private sectors. Financial institutions, universities and many others use the framework today.

Roar Thon, at the Norwegian National Security Agency, is one of the very few experts on security culture. His input, questions and support are always helpful, and his generosity is out of this world. Mo Amin, a London-based security consultant, dedicated many hours of his precious time to review the manuscript and concept for the book. Amin is also a key resource on the Security Culture Framework community, and an inspiration to follow. My thanks also to Wolfgang Goerlich for his helpful comments and feedback during the review process.

A special note to Michael Santarcangelo, who provided deep insights through his questions and ideas. I thank you, sir!

Numerous discussions about security awareness and culture with fine folks such as Javvad Malik, Thom Langford, Quentyn Taylor, Trond Sundby, Rune Ask, Troy Hunt, Joshua Corman, Per Thorsheim and Brian Honan helped me gain an understanding of what security culture is, and how to best bring it about. We may not always agree, but we certainly do learn!

This book would never have been were it not for Joe Pettit at Informationsecurity Buzz. His introductions and continued support has been vital. Vicki Utting at IT Governance has been a great asset when I tore my hair out over writing this book.

To the information security community worldwide: thank you for keeping me on the edge, for challenging my assumptions and for keeping me safe!

Most importantly, thank you to my dear wife, Karolina, and Leo, my son. You are the light.

ABOUT THE AUTHOR

Kai Roer is a management and security consultant and trainer with extensive international experience from more than 30 countries around the world. He is a guest lecturer at several universities, and the founder of The Roer Group, a European management consulting group focusing on security culture.

Kai has authored a number of books on leadership and cybersecurity, and has been published extensively in print and online, and has appeared on radio, television and featured in printed media. He is a columnist at Help Net Security and is the Cloud Security Alliance Norway Chapter President since 2012.

Kai is a passionate public speaker who engages his audience with his entertaining style and deep topic knowledge of human behaviours, psychology and cybersecurity. He is a Fellow of the National Cybersecurity Institute and runs a blog on information security and culture (roer.com). Kai is the host of Security Culture TV, a monthly video and podcast.

FOREWORD

"May you live in interesting times" is an old saying and one that is certainly applicable to cyber security today. As the unfolding events of the past few years have shown us, we are indeed living in interesting cyber times. The evolving cyber breaches of every sector, be it retail, government, education, financial or others, have been the main focus of the technology conversation this entire year. Big box retailers have been hacked, sensitive data at banks breached, and nation states stand ready to wage cyber warfare.

We have developed computers and the Internet and attached many of the most important aspects of our lives to it. Now we find those connections are at risk due to the activities of 'bad actors' bent on malicious activity. We try to defend our digital systems with properly configured soft and hardware, but in the end it is often a 'people' problem that permits a large portion of the breaches we read about. People are just not following appropriate procedures thereby allowing improper access to systems. As many are aware, the best way to reduce human errors we encounter is through effective education and training. Sadly such education and training around the globe is spotty at best and often wholly inadequate.

With this book, Kai Roer has taken his many years of cyber experience and provided those with a vested interest in cyber security a firm basis on which to build an effective cyber security training programme. This requires change, and understanding how the culture of an

organisation needs to change to be effective is vital for cyber success. Each chapter is filled with valuable insights, examples and intuitive thoughts based on his experiences that can easily be transferred to the workplace. As system administrators scramble to harden their respective defences, this work couldn't have come at a better time. Anyone obtaining this book will find it a valuable and informative read.

Dr. Jane LeClair
Chief Operating Officer
National Cybersecurity Institute, Washington, D.C.

CONTENTS

Introduction 11
Culture: Does it have to be so hard? 11
Chapter 1: What Is Security Culture? 15
Chapter 2: The Elements of Security Culture..... 30
Chapter 3: How Does Security Culture Relate to Security Awareness? 36
Attention..... 45
Retention 45
Reproduction..... 46
Motivation..... 46
Chapter 4: Asking for Help Raises Your Chances of Success 50
Chapter 5: The Psychology of Groups, And How to Use It to Your Benefit..... 63
Chapter 6: Measuring Culture..... 77
Chapter 7: Building Security Culture..... 86
Metrics 89
Using SMART goals 91
The Organisation part..... 92
Topics..... 96
Planner 100
Setting up your organisation to use the Security Culture Framework 102
Chapter 8: Time Is on Your Side..... 107
ITG Resources 110

INTRODUCTION

Culture: Does it have to be so hard?

In this book, I look at organisational culture with information security glasses. In my years of working in the information security industry, I have come across a number of challenges: technical, compliance, and increasingly awareness and security behaviour. Through my travels and company activities, I have learned that a lot of security behaviour challenges are universal: preparing information security information in such a way that it resonates and makes sense for non-security people is a challenge no matter which country or organisation you work in.

I have also learned that some organisations are better at creating the security behaviour they want. Looking at what they do differently, I found that they approach the work with security awareness as a process. They also respect that security competence is exactly that – a competence that must be learned, not just something you tell.

From more than two decades of professional training and consulting in more than 30 different countries, I have also come to learn that if we want people to learn, we need to facilitate learning together with them. Lecturing alone is not creating results. Reading alone makes for very little change. The saying of the Association for Talent Development (ATD[1]) that "Telling ain't Training" is very true. It took me some time to realise that I too had to learn

[1] Formerly the American Society for Training and Development (ASTD).

how to train people properly, a realisation that took me on a rollercoaster of learning, exploration and self-development, leading me to develop my training and communication skills across both language barriers and cultural barriers.

The most important thing I learned in these years was to be humble. Humble about my own perspectives – I may think I am right, and I may have all the experience to tell me I am right, but implant me in Tunisia or Japan and most of my perspectives and experience in treating and communicating with people no longer hold. I learned this the hard way, leading me to realise that there are more ways of doing things than I first accounted for, and that others may achieve great success by choosing a different path than the one I chose.

The same is true with organisational culture. There are many ways of building, changing and maintaining organisational culture. It is one of those areas where scientists and practitioners still argue about the right approach[2]. My experience is that the right approach depends on each case. Every organisation is unique and comes with its own culture and subcultures. Some are great, some really poor. All of them impact the behaviour, ideas and thoughts of the employees. The question becomes: how do we take control of that culture?

[2] A quick search through academic papers via Google will amply demonstrate the variety of approaches within academia alone, while a similar review of the titles available on Amazon reveals a similar breadth among practitioners. For a comprehensive review of the topic (and many other topics!), read Bernard Bass' *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications*.