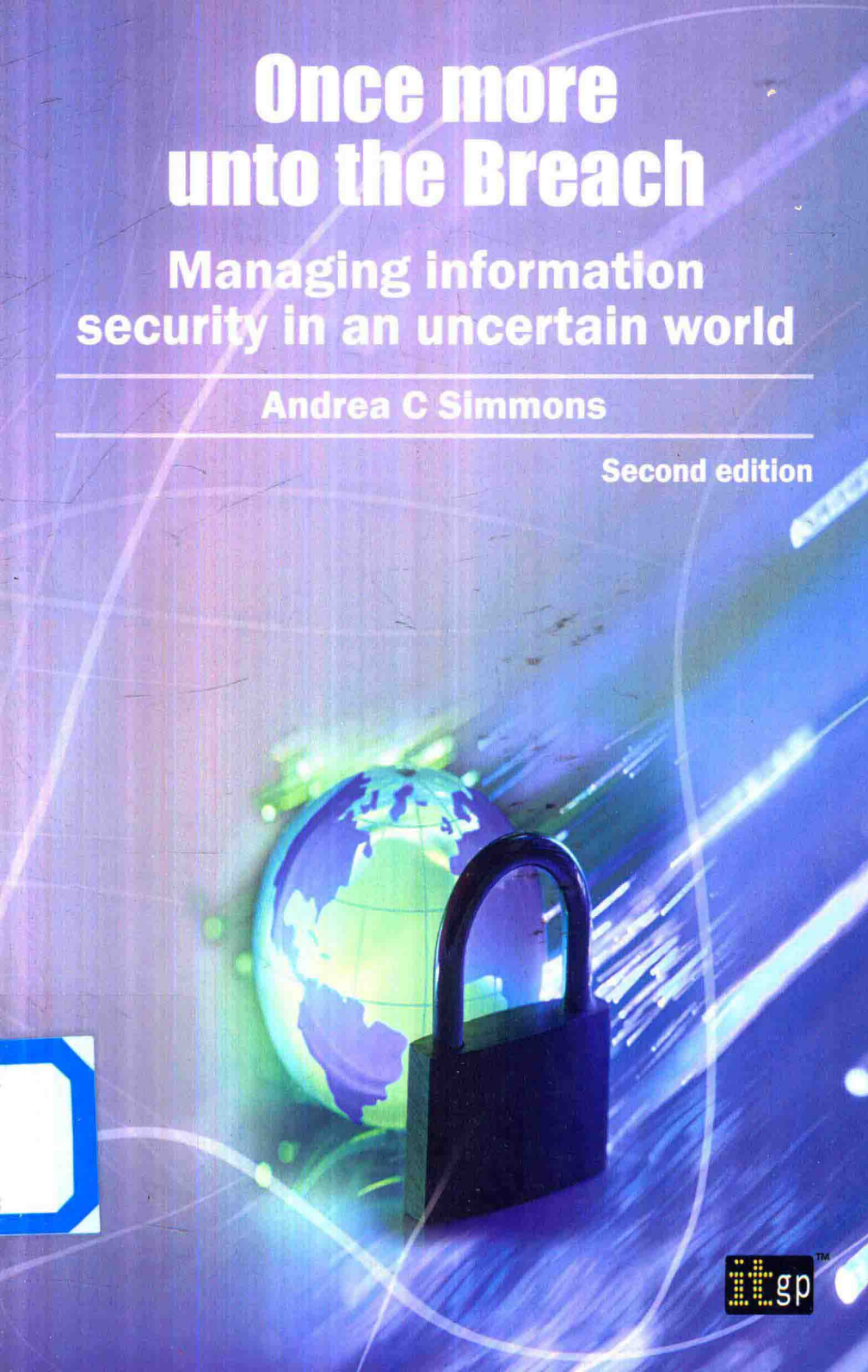
Once more unto the Breach

Managing information security in an uncertain world

Andrea C Simmons

Second edition



itgp™

Once more unto the Breach

Managing information security in an uncertain world

Second edition

ANDREA C SIMMONS

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 2012
by IT Governance Publishing: ISBN 978-1-84928-388-5

Second edition published in 2015

ISBN: 978-1-84928-708-1

Once more unto the Breach

Managing information security in an uncertain world

Second edition

PREFACE

This book was first spawned from years of experience in the UK information security industry, both from being in the role of an information security manager and more recently a chief information security officer, and from observing many individuals adopting the role from a standing start, without making a deliberate career choice or realising that it would be part of their role. Let's be honest, you don't hear many (any?) teenagers planning to leave school to be an information security manager! The role is often 'gifted' (in the poisoned chalice sense!) to an individual on top of their existing, hugely busy, day job, because the person handing over the 'gift' does not understand the breadth of what is required. Therefore, the individual in receipt of the 'gift' is not afforded the time or respect required either to provide appropriate advice and guidance for the protection of information assets belonging to the organisation in question, nor to actively encourage colleagues to do likewise.

The aim of this book is to provide a 'coalface' view of what tackling this role actually looks like in action, drawn from my own experience; having spent a year during my PhD studies taking on the role of information security manager for a UK public sector body, I quickly realised the benefit of keeping copious notes! In academic circles, this is known as carrying out 'participant observation' and was done as part of PhD research into embedding best-practice information assurance. The author observed a great many incidents, events and risks, and also participated in innovative solution creation in order to address all of these.

The results of this study are worth putting together in this tome - almost every day brought with it a little gem which, if you were not 'in tune' with the wondrous breadth of information security, you might have missed, including the cause and the potential mitigation and 'lessons-learned' elements.

This book is effectively written through the spectrum of the 'project lessons learned', which were harshly, but fairly, created after phase one of a long project. Given that this book is based on a real project that took place several years ago, the text is imbued with a great deal of hindsight. However, these lessons could no doubt have been written by many people in any organisation. Part of the author's current research has been looking into the whys and wherefores of how organisations create lessons-learned logs, but do not actually learn the lessons well nor implement the required changes in practices. The work is appropriately anonymised.

While some of these issues and incidents took place between 2009 and 2011 and may feel out of date (given how fast the pace of life is in the information age), you may still be experiencing some of them and the lessons learned will hold true for most situations.

So, I share this with you in the hope that either they will resonate with you and you will feel reassured that you are not insane, or you will start to see things differently and know what to watch out for in the future with enhanced vision.

ABOUT THE AUTHOR

Andrea Simmons, M.Inst.ISP, CISSP, CISM, FBCS CITP, MA, ISSA Senior Member and IISP Director, is Chief Information Security Officer for HP Enterprise Services.

Andrea is an enthusiastic information governance evangelist and specialist with extensive experience in both the private sector and the UK-wide public sector – including local government, non-departmental public bodies (NDPBs), and health and emergency services. Andrea has expertise in information security management systems (ISMSs) (ISO27001, strategy and planning, policies and procedures development and implementation, etc.), information rights legislation/regulation and standards (including data protection (DP) and freedom of information (FOI)), records management (RM), governance risk and compliance (GRC), information assurance (IA), business continuity planning (BCP), resilience and disaster recovery. This covers the breadth of UK public and private sector compliance requirements including ISO27001, FSA, ICO, data handling, PCI, CoCo, GCx, security architecture and design, implementing compliance programmes and ISMSs, through the deliverance of change management programmes and innovative training solutions, while being heavily influenced by US and global legislation, regulation and standards development and maturation. Andrea has been an active information security industry contributor for a decade, writing articles and blogs and presenting at conferences, seminars and workshops.

Andrea has contributed to standards developments and industry research and is now working on a PhD in

information assurance through the University of Wolverhampton, researching the background to the development of the subject itself – its genus and meaning across the industry – and tackling the language barriers created by our complex web of industry acronyms and misconstrued meanings, which appear to be hampering the implementation of best-practice information assurance in the context of the information society.

Andrea has also held the role of consultant security forum manager for the BCS Chartered Institute of IT: *www.bcs.org/security* and is now a member of the BCS Security Community of Expertise (SCoE), and has been a member of the Management Committee of IAAC, *www.iaac.org.uk*, for several years. She is also a full, Chartered Fellow of the BCS and its relevant specialist groups: security, audit and law, and is on the BCS Register of Security Experts. Andrea is also a member of ISACA, ISSA, ISC2 and a founding member of the Institute of Information Security Professionals, to name but a few!

Andrea achieved Chartered IT Professional Status in February 2007 and M.Inst.ISP in 2008. In January 2012, Andrea was awarded Senior Member status of the ISSA, *www.issa.org/.*

ACKNOWLEDGEMENTS

I am indebted to my parents for bringing me up with the strength of character that has made me a relatively open individual, which means that people tend to warm to me, rather than shying away. This can be a helpful trait in the role of information security manager, as you need people to feel that they can trust you and can share whatever issues are taking place that need solutions. I am also grateful to my mother, Jean, most particularly for a love of language and the spoken word – and even more so that she would take the time to read this book, so utterly 'out of the norm' from her normal reading, and find all the little niggles that needed to be ironed out!

I am grateful to all those colleagues I have met in the various roles in which I have been lucky enough to have influence during the last two decades. There really are some fascinating jobs out there, but more interesting yet, from our perspective, has to be how to weave information security into the fabric of what we are doing, to make it live and breathe on a daily basis.

I am also indebted to the various colleagues I have met along the way – in particular, those who are as keen to change things for the good as I am – dedicated to representing information security positively, rather than negatively; sadly, the usual default position. We don't have to be 'the department of no'!

Last, but by no means least, I am, of course, hugely grateful to my husband for putting up with my continuous need to write stuff down!

We would like to acknowledge the following reviewers of this book for their useful contributions: Chris Evans DPSM MBCS and Giuseppe G. Zorzino CISA CGEIT CRISC, Lead Auditor 27001, Security Architect.

CONTENTS

INTRODUCTION

"Once more unto the breach" is a key phrase from the "Cry God for Harry, England and Saint George!" speech of Shakespeare's *Henry V*, Act III, 1598. The breach in question is the gap in the wall of the city of Harfleur, which the English army had put under siege. Henry was encouraging his troops to attack the city again, even if they had to "close the wall with English dead". We read these kinds of battle-cry stories now, in our enlightened and empowered times, and find it hard to countenance such unfailing support for heading into a perilous situation.

As an information security manager (ISM), you enter each day not knowing what it may bring, in spite, perhaps, of a well-formed plan or at least a 'to do' list. Each event or incident that you encounter is only a gnat's whisker away from being a full-scale breach, depending upon your knowledge, skills or ability to cope under pressure. This book is centred in this space and is based on the clear appreciation that there is no such thing as 100% security and you can never be 100% risk free.

From an academic perspective, the author is both examining the historical methodology – seeking to review the history of IA and why it is that there is so little real agreement with regard to a the correct definition – and building a grounded theory, whereby through interactions and research, the author creates a theory and then tests it over a period of time. The author's contention is that it is as a result of a fundamental lack of knowledge that we now have difficulty (and confusion) in progressing to a mature

IA profession. Health warning – I should say up front that this book won't pull any punches.

When this book originally came out, it focused on a period of time between 2009 and 2011. In many media reviews of the time 2011 was hailed as the year of the hacker, in terms of the volume of media coverage and, therefore, widespread global awareness, and was noted to be a year of significant data breaches and losses because of the large numbers of individuals directly affected or impacted. Today we regularly see reports of well-known companies falling victim to cyber attacks, and the situation that seemed exceptional in 2011 has become the norm. In fact, given the volume of breaches experienced since this book was first published, its contents have never been more accurate or more appropriate. 2014 in particular was a year of extreme activity, with vulnerability after vulnerability being experienced across all operating systems – including the first significant chink in the armour of all things *nix (with the Bourne Again Shell – BASH/Shellshock vulnerability). In reality, the breaches that are covered by the media are only the tip of the iceberg, and the longer you work in the industry the clearer this becomes.

Beneath the story reported by the media there is usually a

Security is having a bad decade…..

So many breaches!

10/2014: Home Depot (53m records)
9/2014: Home Depot (56m cards)
8/2014: JPMorgan Chase (83m records)
6/2014: iCloud (celebrity 'hacking')
5/2014: eBay (145m records)
12/2013: Target (110m records)
10/2013: Adobe (152m records)
And on, and on … It's obvious there are some serious issues to be addressed.

raft of information security-based failings that have been present for quite some time.

All of these, one after the other, like multiple buses arriving at the same time, could have been adequately resolved with three key information security management tenets, which are addressed through this book:

1. Inventory management (knowing what you have) [Chapters 1, 4, 7 and 8]
2. Patch management (keeping it up to date) [Chapter 2]
3. Vulnerability management (protecting it from harm) [Chapter 3]

Why is this the case, given that there are likely to have been many valid audit reports containing reference to issues that needed to be addressed? Indeed, there is no doubt that had recommendations been adhered to in these cases, risk reduction would have occurred and the number of breaches would equally have been lessened. It seems to me that, as a society, we have seen a greater shift in recent times towards openness and transparency in all walks of life and across all levels of leadership. I believe we should be following this trend in our own industry.

This book is an insider's view of how many actual breaches (often seen as incidents) are going on all the time, but which do not get reported, either internally or externally. The educational point of the book is to reframe what it actually means to be an ISM, as well as what is meant by an incident, how we respond to it and what the most appropriate reporting and reactions should be. We will do this through the old art of storytelling, in the hope that better informed and more aware ISMs will be able to

provide much greater protection to their organisations and their information assets.

The book will be peppered with references to real issues, conflicts and conundrums that ISMs constantly have to deal with, and I hope that it will shed light on possible solutions and pragmatic ways forward. It should be usable as a learning device and reference guide.

The chapter structure is based on a 12-month chronology, running from August to July.

August – pulling a team together. As a project manager in information security you get what you are given and you have to make the best of it, so you have to enthuse those around you regarding your goals while explaining the changes in behaviour expected and what the end game looks like.

September – street trash. This chapter is centred on an event that may remind you of those times when you read news stories and don't expect them to happen to you. But when you spot the blindingly obvious, always remember to take a photo so you have the evidence to 'show and tell', following the mantra 'a picture is worth a thousand words'.

October – compliance is only skin deep. Once you've completed an audit, in whatever shape or form, following a 'tick box' exercise is no good if you can't back it up with evidence. Now starts the hard work of living by your word.

November – how remote is remote? Identifying home-workers and remote workers can be a tricky business depending on your partners and your boundaries, the competing requirements of each, and conflicting legislative and standard requirements.