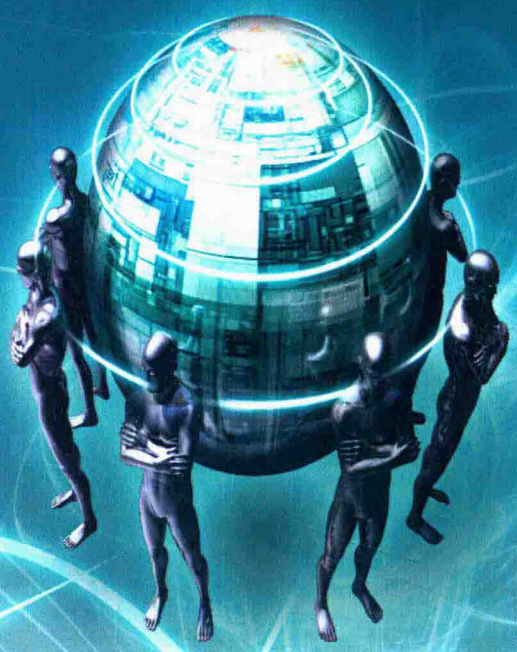
Managing Information Security Breaches

Studies from real life

Michael Krausz

Second edition



itgp™

Managing Information Security Breaches

Studies from real life

Second edition

MICHAEL KRAUSZ

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 2010
by IT Governance Publishing: ISBN 978-1-84928-094-5

Second edition published in 2015
ISBN: 978-1-84928-595-7

Managing Information Security Breaches

Studies from real life

Second edition

FOREWORD

In 1992, a business acquaintance of mine introduced me to something he called 'the ultimate book on information security'. It turned out to be a guide written by a retired NSA officer with a tendency to talk a little bit more than would probably have been allowed in the terms of the NDAs he had once signed. This, of course, was all the more appreciated by those listening to him. The book focused entirely on written information, and had originally been published in the late 80s or early 90s, a time when I started to use punch card paper as notepaper because there was no longer any use for it in the large IT centres. Much as I respected the retired NSA officer, I felt uncomfortable because the book, even though it was only about 20 years old then, was hopelessly outdated and old fashioned. The way of working with information had changed so much since the time it was written that, early on in my career, I felt that I had to look elsewhere for guidance than to retired NSA officers.

Nowadays, with the ISO27000 family, general information and guidance on how to establish and preserve information security (IS) are readily available for purchase. This is not quite the case when it comes to the question of what to do 'if something happens'. Feeling that the market is not properly served, I thought that it would be valuable to provide the readership with insights on how cyber-investigations are conducted, and on what to do in the event of an incident. This book aims to go right to the heart of what needs to be discussed, carried out and learned from an

information security incident, covering the full breadth of issues that arise when the worst comes to the worst.

This guide is aimed at CSOs, CISOs, IT security managers, CIOs and, last but not least, CEOs. It particularly addresses personnel in non-IT roles, in an effort to make this unwieldy subject more comprehensible to those who, in a worst-case scenario, will be on the receiving end of requests for six- or seven-figure excess budgets to cope with severe incidents.

This edition has been updated to reflect the transition from ISO27001:2005 to ISO27001:2013. All content related to or referring to "ISO27001" is in accordance with the current version, ISO27001:2013.

PREFACE

The aim of this book is twofold. Firstly, it provides a general discussion of what information security breaches are, how they can be treated, and what ISO27001 offers in that respect, illustrated with details of real-life information security incidents and breaches.

Secondly, it will form a 'first line of defence' for the reader who is affected by an incident and is looking for guidance and direction.

The Pocket Guide companion to this book summarises all the major points and aims to be a concise reference work for the avoidance and treatment of information security breaches. This book, however, deals with the aspects of information security breaches in extensive detail, with an emphasis on the word 'extensive'. The author wanted to make sure that nothing was overlooked, and everything is explained down to the last nut and bolt – or, at least, the last nuts and bolts that can still make a difference to the final outcome of a breach.

You do not have to read the book strictly from beginning to end. You could start with the case studies in Part 2 for some real-life scare stories, then proceed to Part 1 for a structured overview of risk management, followed by Part 3 to study a sample treatment process. The sequence followed by the three parts of the book, however, leads the reader from learning what is relevant about risk in general, to real-life stories about risks that have materialised, then going on to learn what can be done to effectively and efficiently handle breaches once they have materialised.

ABOUT THE AUTHOR

Michael Krausz studied Physics, Computer Science and Law at the Vienna University of Technology, Vienna University and Webster University. Combining his two main hobbies, investigations and computers, he has, over the last 20 years, become an accomplished professional investigator, IT expert and ISO27001 auditor. He has investigated over a hundred cases of information security breaches, usually connected with varying degrees of white-collar crime.

He has delivered over 5,000 hours of professional and academic training, and has provided consulting or investigation services in 21 countries so far.

ACKNOWLEDGEMENTS

I gratefully acknowledge the assistance of IT Governance Ltd, without whom this book would not have seen the light of the bookshelf, real or virtual. I would also like to acknowledge the direct or indirect support of friends, colleagues and business partners. Special thanks go out to Chris Evans and Michael Wang who both provided much cherished feedback on the first version of the original manuscript. Further thanks should be extended to Angela Wilde for managing the first edition of this book and to Vicki Utting for managing its second edition.

Alan Calder and Steve Watkins of IT Governance were essential in bringing it to life in the first place by acknowledging that this somewhat uncomfortable subject needs to be tackled.

CONTENTS

INTRODUCTION

Breaches of information security are not a new phenomenon, but the means of perpetrating such breaches have changed considerably over the years. Leaking information has always been an issue, but the speed and effectiveness with which breaches of information security can occur, and the potential magnitude of harm caused in today's computer age, are disturbing and, moreover, typically favour the perpetrator, not the victim.

Bearing in mind the dependency of modern companies on their IT systems, it is clear that special care needs to be taken to keep systems safe and secure. This book focuses solely on the aspects of re-establishing safety and security once, despite all measures taken, a breach has occurred. It puts breaches of information security in the context of ISO27001 which, since its inception in the late 80s as British Standard 7799, has demonstrated that it can provide a framework of requirements well suited to the effective implementation of countermeasures and measures designed to protect information in all its forms, whether on paper, in speech or in the IT field.

This book describes a process and its elements for the treatment of severe breaches, and places them in the context the relevant ISO27001 controls. It provides input for decision making and for breach classification, and offers case studies to enable the reader to explore how other companies were affected and what they did (or did not do) upon falling victim to a breach.

These case studies have been carefully selected from the case collection of the author, and some cases have been

included that entered the public domain, but where the author has background knowledge. Naturally, some facts regarding the identities of companies and locations had to be changed to protect the companies and their business. All the basic facts relevant to the breach and to each case are true, and happened as described.

This book is structured along a precise line of thought: definitions and general subjects in Part 1, real-life case studies in Part 2, and what to do to resolve a breach in Part 3.

Part 1 serves as an introduction by defining the terms 'risk' and 'breach' and putting them into the context of a risk management framework, as well as describing general avoidance strategies as contained in ISO27001. This part can be seen either as a means for the reader to complement existing knowledge, or as a starting point for those who have not yet delved deeply into matters of risk management.

Part 2 comprises a number of case studies to provide the reader with real-life stories of breaches and subsequent events. ISO27001 even states that a company should try to learn from its own incidents and those of others. This, in the real world, turns out to be rather difficult as companies have a natural tendency not to be too open about such incidents. The author feels that we are closing a gap with these case studies, all of which have been taken from a collection of more than 100 cases in which he was personally involved. Part 2 describes the events, and includes a full explanation of what actions were taken, why, and what the outcome was, including lessons learned.

Part 3 provides a sample treatment process in descriptive form.

PART 1 – GENERAL

CHAPTER 1: WHY RISK DOES NOT DEPEND ON COMPANY SIZE

What is the real worth of the USB stick you just bought for £15? After a year, if you included it as a short-term cost item in your accounts, it would not be worth anything. On the other hand, if it contained all the latest data of your research project which was bound to pay off in a couple of years, then it would be worth pretty close to infinity or, at least, the future of your company.

It is not easy to define risk or what taking a risk really means. Sometimes people try to use probabilities and ALEs (Annual Loss Expectancy); sometimes damage or the propagation of damage along a business process is included; sometimes risk is described as a vector of vulnerabilities and threats (which is the favoured way to see it in the information security world); and sometimes it is described by the options available for action. We will not try to give you a comprehensive, all-encompassing definition. We just want to make a couple of points: that risk permeates your company or corporation from top to bottom, from head to toe and, particularly, that risk and information security risks do not in any way depend on the size of your company.

This latter point is important, as companies sometimes tend to underestimate their exposure and to overestimate their resiliency (cf. 'too big to fail' as a banking sector

paradigm). There is no such thing as 'too big to fail' in the information security world; a well-organised incident can bring down empires or, at least, damage them so much that recovery can take years, if it even remains affordable. It is true, however, that there are distinct differences in how companies can cope with, and avoid, incidents. Some avoidance and treatment options are largely based on size, but, then again, size is measured here as in 'cash available', 'reserves available', 'speed to implement treatment options', and so on. Company size, measured, for instance, by number of employees or locations, does not really mean anything in regard to information security risks.

Let us briefly state the definition of company sizes as used in this book. For our purposes, a company with up to 100 employees is considered small; 100 to 1,000 is considered medium; and 1,000+ is considered large. For the sake of clarity, we will not take into account revenues, cash or profits, and we will not consider that these sizes may all be considered small in some countries or may fit another country's business structure perfectly. As a real-life example, consider an actual company in the medical sector, with only 300 employees, that makes more than a billion euros a year selling its specialised devices.

Let us, first of all, give a brief definition of risk in the information security world. The most commonly used, most practical, approach today is to define risk as a vector of vulnerabilities and threats, with some likelihood and damage levels associated later. A vulnerability is a weakness that can be exploited by an associated threat and is based on properties of the system(s) and process(es) you are using. Vulnerabilities are inherent in IT systems, your physical location, and your processes, because of their design and their inherent characteristics.

A threat is an event or process that can (ab)use these vulnerabilities to cause harm to the confidentiality, availability or integrity of your system (all assets considered as one) or systems. A threat can be man-made or natural; its associated damage can be caused by malicious intent, by accident or by technical failure.

If a vulnerability has a corresponding threat, then a risk clearly exists. The level of risk will depend on the measures already in place, and will be higher, the less effective these measures are. If a vulnerability does not have a corresponding threat, or if a threat exists, but without corresponding vulnerability, then the risk resulting from such combinations is simply zero. Once it has been determined whether a risk exists or not, one will usually factor in the following:

- the likelihood of the risk materialising;
- the direct damage caused by the risk materialising;
- indirect damage throughout a chain of business processes;
- the cost of mitigating measures;
- business priorities of mitigating measures.

In bringing together all of the above, a risk analysis is duly completed (more on that in the following chapter) which will show management what the situation of the company is, and what can be done about it in both the short and the long term. But, to return to the subject of this chapter, none of these factors depend in any way on company size. There is only one question of paramount importance that illustrates our point:

How much damage will this particular risk do to my company?