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 978-1-84928-095-2

Second edition published in 2014
ISBN: 978-1-84928-596-4

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NSA officer, I felt uncomfortable because the book, even though it was only about 20 years old then, was hopelessly outdated and old fashioned.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.

CONTENTS

Introduction **1**

Part 1 – General **3**

Chapter 1: Why Risk does Not Depend on Company Size **3**
Risk effect 8
Propagation of damage (downstream effects) 8
Culture 9
Information security staff 10
Cash reserves / cash at hand 10
Ability to improvise / make quick decisions 11
Preparedness 11
Contacts with authority 12
Chapter 2: Getting your Risk Profile Right **14**
Intuitive risk analysis 15
Formal risk analysis 17
Residual risks 39
Chapter 3: What is a Breach? **42**
Confidentiality breach 44
Availability breach 45
Integrity breach 46
Chapter 4: General Avoidance and Mitigation Strategies **53**
Introduction – general aspects, avoidance and related ISO27001 controls 53
People 54
Processes 69
Technology 78
Strategies and tactics for treating breaches 87

Dimensions of treatment / mitigation of information security breaches 94

Part 2 – Case studies 98

Chapter 5: Notes from the Field 98
Privacy 98
Cost 99
The practicalities of surveillance 99
The truth vs. company policy 101
Chapter 6: Motives and Reasons 102
Greed 102
Despair 103
Revenge 103
Business advantage 105
Chapter 7: Case Studies from Small Companies 108
Foreword to the case studies 108
The stolen backup 108
Eavesdropping on faxes 112
A stolen laptop 114
Chapter 8: Case Studies from Medium-sized Companies 119
A case of intrigue – the missing contract 119
The sales manager who changed jobs 123
The project manager who became a friend, and then an enemy 127
The lost customers – how a sales manager cost a company 10% of revenue 132
The flood – how not to learn about risk management 138
Chapter 9: Case Studies from Large Corporations 142
Who wants my data? – a case of data theft 142
Who wants my data? – a more complicated case 149
Hard disk for sale – beware of your contractors 158

Unauthorised domain links – it is easy to harm a company's reputation 161
The trusted guard who was not 164
Insider badmouthing 167
The software vulnerability that was not – a case of blackmail 169

Part 3 – A Sample Treatment Process 175

Chapter 10: A Sample Treatment Process 175
Step 1 Gather information 175
Step 2 Determine extent and damage 177
Step 3 Establish and conduct investigation 178
Step 4 Determine mitigation 179
Step 5 Implement mitigation 181
Step 6 Follow up on investigation results 181
Step 7 Determine degree of resolution achieved 182
Abbreviations and Acronyms 183

ITG Resources 184

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?

If you look at some risks, for example, the German Baseline Protection Manual's list of threats and vulnerabilities, you will find that some risks can hit you severely, while others are irrelevant, but none of these will have anything to do with the size of your company.

Some risks are almost trivial, such as a CEO's child running some CD in the office and unwittingly importing a virus; some risks are elaborate and require malicious intent, such as social engineering or corporate espionage; but, as this example shows, it could happen anywhere, and it could do the same fundamental damage to any type of company (though larger companies tend to be better prepared).

Consider research-driven companies for a moment. There are large pharmaceutical companies and technology businesses that invest billions in research, and competitors who think that stealing, rather than investing, would be a good strategy. Hence, a threat for the former companies exists. But there are also a number of medium-sized companies who are leaders within their niche, invest heavily in research on a slightly different scale of millions instead of billions, and therefore have the same fundamental risk profile. Based on their cash reserves, a medium-sized company may even be better equipped to survive a fundamental information security breach; in general, though, the level of preparedness tends to be less evolved, but, nevertheless, the nature of the risk is exactly same and, on a carefully chosen risk level matrix, the risk level would most probably also be the same.

So far, we have focused on the effect of the risk in relation to the company, and demonstrated that the risk does not

depend on the size of the company. Let us look at another aspect: preparedness.

Preparedness for an incident depends not on company size, but, rather, on its culture. That culture can be highly evolved or not present at all, but, again, it will not depend on size. In smaller companies (fewer than 1,000 employees) company culture can be much more refined, and can be carried by a mid-level of highly motivated managers who identify with, or admire, the founder or founding partners. In such companies, personal contact with the owner or founder usually occurs regularly. On the other hand, larger companies (over 1,000 employees) can easily evolve into bureaucracies, where people do only what they are asked to do. In such a culture, establishing a new view on risks, or security as a whole, is difficult and can take some time (often up to two or three years). Furthermore, larger companies have a tendency to underestimate the value of building awareness, and concentrate on measures they perceive as being more cost efficient or just cheaper. For example, one defence sector company thought that, instead of a fully-fledged awareness programme involving classroom training and Q&A sessions, handing out CDs and making staff take an online exam would be enough. Unfortunately, this is not always the best way in which to pass on this kind of information.

Next, we will look at the relevant factors for treating or avoiding information security incidents, and examine whether any of these are connected to company size.

Risk effect

As mentioned above, risk effects do not depend on company size for severe risks. Big companies usually do better at keeping a risk from spreading all through the company (downstream effects), but this is countered by the ability of small companies to act promptly and without much bureaucracy. If we measure the risk effect in qualitative terms from 'low' to 'substantial' to 'extreme', then a risk can hit all types of companies equally hard.

Small companies are often less well prepared, and do not quite structure their efforts, adopting a more ad hoc approach, so the effects on them tend to be more disruptive and less controlled than in larger companies which have implemented a fully-fledged information security programme. If we focus on the general effect of any given risk, however, the effects and their range are strikingly similar.

Propagation of damage (downstream effects)

Propagation of damage occurs when damage caused by a risk that has materialised propagates through a business process or a number of business processes. Bigger companies tend to have an advantage, as their business processes are generally more tightly controlled, whereas smaller companies usually face severe customer *chagrin* and loss of business if damage propagates through a chain of processes. As an example, consider the following scenario.

A medium-sized bakery produces bread to be used by a fast-food company. Imagine one of the baking machines not working, due to some IT failure. The bread will not be

delivered and, apart from fast-food customers staying hungry (or eating healthily for a change), contractual penalties may be invoked, further elevating the damage level caused by risk materialisation.

In the automotive industry, a failure at one supplier can propagate through the entire chain of production, causing a standstill at the main factory.

Culture

How risks are seen and treated before they actually materialise is based on a company's culture. In smaller companies, the culture is directly carried by the opinions and attitudes of the IT manager, the managing director, or the owner(s). If the IT manager (there are often no separate IS staff) is on top of their game, this can be advantageous; but if the company still thinks IT is a nuisance as a whole, the result can be totally detrimental.

Having paid the price of establishing their culture through a year-long process, larger companies tend to have the advantage of a more stable culture, which is less dependent on the individuals carrying it; however, even large companies can have an incomplete, or totally absent, view on information security risks, which will then aggravate risk effects.

Again, size does not matter at all, as the culture required to avoid and treat breaches either is, or is not, there. It does not really matter where it came from, but only if it is actually there.

Information security staff

This is the one case in which big companies clearly win. Smaller companies tend not to have IS teams. If you are lucky, you will find a dedicated IT manager for whom, in very small companies (less than 100 people) this may even be an extra role. You will not usually find dedicated information security staff at small companies. Bigger companies generally set up entire teams of information security experts and, today, in a company with 2,000+ employees you can expect to find 3 to 15 people working exclusively on information security issues. One of these people is likely to have some background in investigation, which will prepare the company better for treating a breach.

Cash reserves / cash at hand

One of the most important things in treating a breach is to have quite large amounts of cash at one's disposal, in order to be able to start investigations quickly or to buy equipment to resume operations. The amount of money set aside as reserves or in hand, however, does not necessarily depend entirely on company size, as some small companies may have business models that allow them to have large amounts of cash at their disposal, whereas a large company may find itself stripped of cash due to some other business event or a general lack of free cash flow. Larger companies are more likely to have large reserves, but that cannot be taken for granted. In terms of available cash, successful medium-sized companies, which have managed to secure their niche, are generally even richer than bigger companies.

Ability to improvise / make quick decisions

This is a winning point for smaller companies as, out of necessity they tend to be better at improvisation after a disaster than large companies, which need any number of signatures to get even simple things done. At the end of the day, if disaster has struck, the ability to improvise will again depend on a company's culture, so even a large corporation may show a remarkable ability to work outside the standard band of business processes. Under no circumstances, however, should you think that breaches can be dealt with by shooting from the hip. The basis is always a defined treatment process, but people need to have the ability to think 'outside the box' to solve those problems during a breach that cannot be, or has not been anticipated.

Some companies have processes in place that allow emergency-appropriate temporary shortcuts or a business continuity setup (usually mainly for availability), which allows prompt decision making to speedily mitigate the consequences of a disaster.

Preparedness

The bigger companies tend to win out here, as they usually implement information security awareness programmes and have dedicated staff on their payroll. Smaller companies have a tendency to rely on ad hoc problem solving. They do not usually have processes in place to cope with an information security breach, so they need to rely on improvisation. Of course, the above only holds true if the relevant processes are actually in place, which cannot be taken for granted, even though ISO27001 has passed its

30th year (starting as BS7799 in the late 80s). In other words, larger companies tend to have some advantages over smaller companies, provided said processes are actually in place and operational.

Contacts with authority

In some incidents, such as executive abductions, blackmail or larger cyber crime cases, intense contact with the authorities is necessary, to co-ordinate internal and external activities and to remain on top of the latest news and events in the case. Larger corporations usually have former investigators, or other law enforcement people, on their staff which makes contact with authorities easier. Smart smaller companies tend to look for people with an extensive law enforcement background and lots of contacts to fulfil a security function, whereas the standard small company will be disadvantaged due its lack of staff and of experience in dealing with breaches.

In summary, then, risk does not depend on company size, because:

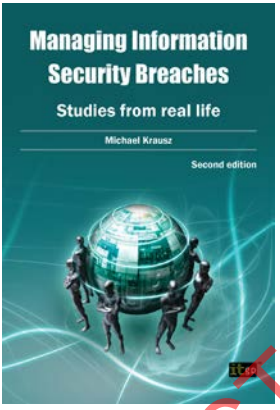
- risk effects can be equally devastating to all sizes of company;
- a culture for treating breaches effectively and efficiently either is, or is not, present;
- cash available depends on the company's financial success, not its size;
- the level of preparedness can vary considerably between companies of similar levels.

At the end of the day, the elements above will define how well a company can handle a breach, and whether

or not it survives the breach in the short term and over a longer period.

<<< END OF EXTRACT >>>

Managing Information Security Breaches: Studies from real life



The book provides a general discussion and education about information security breaches, how they can be treated and what ISO 27001 can offer in that regard, spiced with a number of real-life stories of information security incidents and breaches. These case studies enable an in-depth analysis of the situations companies face in real life, and contain valuable lessons that your organisation can learn from when putting appropriate measures in place to prevent a breach.

Buy your copy today

www.itgovernance.co.uk/shop/p-923-managing-information-security-breaches-studies-from-real-life-2nd-edition.aspx

www.itgovernanceusa.com/shop/p-923-managing-information-security-breaches-studies-from-real-life-2nd-edition.aspx

www.itgovernance.eu/p-516-managing-information-security-breaches-studies-from-real-life-2nd-edition.aspx