Security De-Engineering

Solving the Problems in Information Risk Management

IAN TIBBLE

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
Version Date: 20110815

International Standard Book Number: 978-1-4398-6834-8 (Paperback)

Library of Congress Cataloging-in-Publication Data

Tibble, Ian.
Security de-engineering : solving the problems in information risk management / Ian Tibble.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4398-6834-8
1. Business enterprises--Computer networks--Security measures. 2. Information technology--Security measures. 3. Data protection. 4. Computer security. 5. Database security. I. Title.

HF5548.37.T53 2011
658.4'78--dc23 2011033830

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Introduction

This book is only worth writing because of the nature of human beings and the fact that we will continue to commit acts of deception and aggression against each other for at least the foreseeable future.

The main driver behind the undeniable spike in malevolent activity on the public Internet during the past few years has of course been economic. One could be forgiven for thinking that greed is interwoven into our DNA, so I am not sure that I can say that I would prefer a world without greed because that world is a hard one to picture. A world without human greed is a way different world.

Without greed, there would be no raison d'être for a book such as this one, or any other security books, or indeed security itself. So just for now, we will celebrate humanity and greed because without the latter, there would be no information security. That does not mean I celebrate greed—I am just one of the few in security who actually sort of like my job.

There is a consensus among information security professionals that the picture with regard to global security incidents is getting worse. Reports of information security problems are making headline news with increasing frequency. There are of course sources of information on the actual numbers of recorded incidents, such as Carnegie Mellon's CERT Coordination Center, but one does not need to see the numbers (the accuracy or usefulness of incident data in general is discussed in Chapter 8) to be aware of the increasing scale of the problem. Statistical analysis of security incidents has never been a precise science, and why would an organization wish to report an information security incident if it results in a loss of reputation? Other problems exist with the “science” of gathering breach data, and these are discussed in Chapter 8.

I first noticed a major headline in the *Financial Times* (*FT*) newspaper (not a front-page headline, but a major headline nonetheless) in 2006 about IT security incidents and banks in Japan. “Interesting,” I thought, because it is a widely known fact that as a percentage, more Japan-located organizations subscribe to ISO 27001 (or its predecessor BS7799) than in any other country. Since that article from 2006, there have been more *FT* articles related to breaches and other problems. There have been more articles and reports from all major news sources and with increasing frequency. Certainly when we consider the *FT* and its target audience, it is interesting that major headlines about security incidents are increasingly a common sight.

The U.K. government’s Office of Cyber Security and Information Assurance in 2011 estimated the cost of cybercrime to the U.K. economy at more than US$40 billion per annum.

Incidents in the wild involve attacks against corporations (some of the more common incidents from 2010 to 2011 were related to APT attacks and corporate espionage incidents, the latter of which are usually attributed to Chinese sources) to identity theft attacks against large numbers of individuals. Attacks can be manual attacks by motivated individuals and the more common case: wide scale automated malware attacks. It is really the nature of the attacks that has changed, more than a weakening of security postures. Motivations these days are more financial than before. Back in the good old days, vanity was the more common driver behind malware development efforts.

I would not venture to say that the security posture of networks has improved significantly with time. I do not have the figures because they are not freely available to me, and I do not want to pay for such information, but from my perspective, it seems clear that organizations are now spending more (as a percentage of their IT budget) on information security as compared with during 1998. Does this mean that security postures have improved? Do organizations now have the right balance of risk and spending? The answers to these questions are both “no.”

Among other activities on the “dark side,” thousands of compromised computers in homes and offices are unwitting components in the propagation of electronic crime. “Botnets,” as they are known, are hired out by criminal gangs for those who wish to spread SPAM emails and perform other acts of electronic crime, in such a way as to make the actions hard to attribute to an individual entity. When computers are compromised these days, it is often not noticed by the user because the computer is only used to send spam emails. “Only” used? It sounds like a trivial annoyance—but if it is a corporate computer and it is sending spam, it could result in the organization being blacklisted by other companies.

Organizations on the dark side reportedly exist with management structures and organization charts. There is a supply–demand economic model in the world of selling stolen identities and credit card details. At the time of writing, prices for credit numbers were subject to deflationary pressures resulting from an oversupply of stolen details. According to a Symantec employee: “. . . what can you buy for $10 in 2008? I could buy just under three gallons of gas for my car, which would probably last me a couple of days. I could buy lunch at the local sushi place but only lunch since there wouldn’t be enough left to buy something to drink. Or, I could buy 10 United States identities.”

In January 2010, Google was subject to an incident that may have led to the compromise of their crown jewels—the source code of their search engine. Later in the year, several tech sector companies (including Google) added new warnings to their U.S. Securities and Exchange Commission filings, informing investors of the risks of computer attacks.

The time of takeoff for the public Internet was around the mid-1990s, and between that time and approximately Q1 2002 (give or take three quarters), information security was the best and most interesting field of information technology. During this period, professionals from different IT backgrounds were attracted to the field. Information security was seen by many as the most interesting IT field. What happened after this period is one of the main themes of this narrative and helped to lay the foundations for the increased frequency of security breaches and identity thefts that we experience at the time of writing.

Many explanations are touted for the rise in occurrence of information security incidents. Most of the explanations that find their way into books such as Bruce Schneier's *Secrets and Lies* and *The New School of Information Security* (Adam Shostack and Andrew Stewart) are perfectly valid, and certainly I can say that unique ways of looking at the problem are described in those books. Also of worthy mention are most of the comments in John Viega's book, *The Myths of Security.* I find congruence in many of the points raised in the aforementioned titles, as well as give my own two cents worth to the industry; I also seek to build on others' comments and give them added momentum—for the good of the infosec industry and therefore the interconnected world in general.

On the aspect of how to deal with the problem, there has also been an increasing volume of big picture solutions—each as revolutionary and incredible as the next, and each composed by management-oriented figures with an approach toward the technical side that borders on disdain. Yes, economics is a factor. Yes, people are a factor (employees in any size of organization must be mandated to buy into a security awareness program and sign off on an information security policy). Yes, we need to improve our "processes" and other factors that have different names but mean the same thing.

The noble efforts of various figures in the information security community to remind the world at-large of these risk-mitigating factors are much appreciated by at least the author of this narrative and hopefully also C-level executives.

Local Stories, Global Phenomena

In my journeys as an information security professional, I have had the privilege to work with some of the best in the industry and the worst of the worse. I have encountered stories from all areas of the spectrum that are not for the faint hearted.

In my work with various Fortune 500 clients, I grew sufficiently acquainted with their business and IT practices that I was able to get to know their personnel issues and see in detail how they went about trying to handle information security.

I have spent weeks, and in some cases months, with clients, mostly in finance, but also transport, insurance, tobacco, electronics, and logistics. I worked full-time with two major consulting firms and one multinational insurance company. My other engagements were as a contracted consultant to a variety of companies, in offices on three different continents.

Over a decade, I have grown to become familiar with some common trends that I see across companies and continents. These are not trends that are particular to a geographic or industry sector. The problems I illustrate are global, and they are, in my opinion, the problems that are the root of all evil in today's information security practices.

Some of the phenomena I describe in this section, and others, will surprise many readers in that they have personally never experienced such phenomena. Some will be aware of some of the problems I describe, but have never witnessed a description of the problems in black and white. Others would see what I have written and be of the conclusion that the problems I describe are subjective and only exist in a limited sample of organizations.

I have witnessed global-scale information security practices across the globe, and I mentioned my vocational exposure so as to re-enforce the point that the observations I illustrate in this book come from similar experiences in *every* organization with which I have been acquainted. And to emphasize again, in case it was not clear before, that is *a lot* of organizations. Given the fact that my observations are common to all organizations, with the possible (but unlikely) exception of a very small percentage, we can say that these symptoms are indicative of an illness in today's world of commercial information security.

In the earlier days of my career, I was shocked at some of the practices I witnessed in supposedly reputable multinationals. I also was under the impression that what I saw could not possibly be symptoms of an industry-wide pandemic. But then as time progressed, I began to realize that what I experienced was in different ways common to all organizations.

With this narrative, I do not aim to shock. If my intention were really to shock readers, I would probably have written a horror story. Some will read this and be horrified by its content, but it was not my intention to keep people awake at night. If some readers have trouble sleeping at night as a result of reading my diatribe, then I most humbly apologize. Let me reiterate: that was not my intention. As I said before, sometimes you have to be cruel to be kind. Of course my book may also have the undesired effect of inducing sleep as opposed to preventing it.

My career as a consultant started out in the Asia–Pacific region. Our head office was located in Bangkok, Thailand. Most of our clients were based around the region in places like Singapore, Taiwan, Hong Kong, Malaysia, and Indonesia, with some smaller involvement in the local Thai market. Later we started to get more active in Australia.

There were a few occasions where I was required to visit our HQ in Herndon, VA. Our U.S. regional office served the needs of literally hundreds of clients across the length and breadth of the United States.

From that company, I moved to work full-time as an analyst with a global logistics giant. Their regional "Information Technology Service Centre" was located in Prague, Czech Republic. During my time as an associate director with a "Big 4" consultancy, with a centralized global support team, I came across many reports and stories pertaining to client audits from just about everywhere that you can imagine. Later in my career, I was based full-time in London as an analyst with a multinational insurance firm.

So from diverse global experiences, I expected to hear diverse stories in terms of client awareness and the level of maturity of security practices. I was totally wrong. In fact, I heard the same stories from all areas. I expected the U.S. clients to be more aware and more risk averse. They were not. The analysts in our HQ in Herndon had the same war stories to tell as we did in Asia–Pacific.

The Devil Is Everywhere, Including in the Details

The overall momentum since the earlier part of the "noughties" (2000 to 2010) has been away from technical solutions and technical people. Many professionals in security see the battle lines as being drawn in the area of employees' security awareness. Granted, this is certainly an area of concern. Companies can implement the most balanced, cost-effective, perfect technical security solution and manage the infrastructure superbly, but if an employee discloses their corporate logon password to the wrong person, the results can be economically catastrophic for the company.

Issues such as user awareness, implementation of international standards, and information security management systems are critical issues that cannot be ignored, but in the architecting of IT security solutions, it should not be forgotten that there is a technical element to the solution. Hackers play on a technical playing field, and for this reason, security professionals also need to play on the same field. Not everyone can be a manager on the sidelines.

Given all the talk of Internet user awareness and so on, one could be forgiven for thinking that the world has successfully negotiated the whole area of technical vulnerability management (and more generally the ISO 27001 domain "Operations and Communications Management"). Make no mistake, the subject of IT risk management is not entirely a technical area, but there are many "out there," some of them security professionals with 10 years or more experience, who succeed in convincing the budget approver that the solutions are entirely composed of "processes" and "awareness," and the solutions can be implemented with minimal, transparent use of technical input.

The processes, management, and the awareness of the "average schmoo" are important elements to consider, but they are not more or less important than the other oft-neglected sides of security.

Security Is Broken

When discussing the information security sector, the word "broken" crops up quite often in blogs and other sources. John Viega is chief technical officer (CTO) of the Software as a Service (SaaS) business unit at McAfee (now Intel), and in his book *The Myths of Security* he says about security: "A lot of little things are just fundamentally wrong, and the industry as a whole is broken."

With today's social paradigms, there will always be someone, somewhere who sees use of "broken" as a descriptor for the security industry as "cynical" or "nonconstructive." Apparently, we need to be more "positive" in our assessment. Such responses are quite often born from insecurity and a defensive mindset, but then there are also those who are permanently in "glass half full" mode.

Others have said that the industry is not broken; it is just going through a growth phase. "Security is *immature*?" The industry *is* immature, but is it also becoming more mature with time? The answer is unequivocally "no."

I discuss such points as drivers for security spending in the first chapter of this book. Are there drivers out there that would lead to better security and more efficient use of corporate resources in information risk management? Right now, I do not even think we can see the problems clearly, and the first step of solving a problem is the realization of its existence. So there are no drivers for improvement at this time.

When you have a poor state of affairs such as this, with no visible signs of drivers for change, then "broken" is a perfectly fine phrase to use.

Leave the Details to Operations?

If we look at a short case study that involves a risk assessment with a database, the nontechnical security staff will see the database according to the dictionary definition, something like a store of logically organized information. They may see the database as being fixed in the network somewhere, but it is not in their mandate to analyze risk using nasty network diagrams, data flows, and so on.

A database is a collection of information that can be represented in successively more detailed layers of abstraction down to bits as in zeros and ones. The data are organized by a software package such as Oracle or MySQL Server—a relational database management system (RDBMS) package. The RDBMS is hosted on a computer (or "server," as in the classic client–server model) that will run an operating system (OS) such as some flavor of Unix or Microsoft Windows.

The server is physically connected to the rest of the network, usually with an Ethernet cable that links to a hub or more likely a Cisco switch (Cisco has a greater market share as opposed to another manufacturer such as Juniper). That switch is in itself a CPU-controlled device with an OS, much like a computer, that can be configured in many different ways.

The switch is connected to a large corporate private network with (hopefully) firewalls and other network infrastructure devices. OK, so you begin to see the picture develop. How do we assess the risk in this case? The *devil is in the details*, as Bruce Schneier has commented. In order to know the risk, we need to know the risk associated with each device in the connection chain from the "outside" (the public Internet) to the database server, and then even on the database server itself—how would a remotely connected individual first compromise the server and then the information it hosts? What are the threats and *attack vectors*? There is in many cases a greater risk from the internal network as compared with external, although at the end of it all, a network is a network.

I think it is clear that in order to assess the risk to the database, the skills required are both technical and diverse, but the stark reality is that in most security departments I come across, there may be one or two who have a background in IT administration, or they "have a Linux box at home." The skills required to effectively assess risk do not exist in the vast majority of security teams in large companies, but it is their mandate to assess the risk.

Some security teams "teflon" (a commonly used phrase, at least in the U.K., which means nonstick) the risk assessment to operations. Yes, the operations teams are more technically versed, but does the skills portfolio of a typical operations team cut it when it comes to risk assessment here?

In Chapter 4, I discuss the commonly held premise that the nasty technobabble stuff can be dumped on IT and/or network operations departments.

There are certain rarefied skill sets that died out in white hat/ethical corporate environments years ago. These are the skill sets necessary to carry out a risk assessment. What are the required skills exactly? Security departments need a portfolio of skills, the contents of which are summarized in Chapter 11.

The Good Old Days?

Since the early 2000s, things did get less "engineeringy" or "de-engineered." Since that time, security did become a nonfunctional waste of corporate resources. But that is not to say that things were perfect in the mid to late 1990s. No, far from it—in fact, there was a major ingredient missing in those days and that was the "f" word—finances. Small details!

So really, all that old technical speak was of no more value than today's IT-free security offerings from corporate security teams.

Whereas the advisories from the good old boys were factually correct, the efforts were misguided, too much or too little attention to detail was applied to every situation, and the whole effort lacked the necessary direction. Just as an artist has an agent to help them sell their work, the Hackers (I introduce the "Hacker," uppercase "H," in Chapter 2) needed a manager who understood business goals, costs, and architecture, who could maintain good relations with other departments, and who could also manage a small group of highly talented individuals (who could walk out of their job and into a new job in a heartbeat). No such managers existed; moreover, there was no identified need for such a job description.

Some could be mistaken along the lines that this book is purely a critique aimed at the nontechnical elements of the new school. It is not. It is the job functions and skills (or lack of) in vocational security that are several degrees off from where they should be, but that is not to say that things were all rosy in the late 1990s.

The Times They Were a-Changing

In Chapter 4, I discuss some of the changes I noticed happening in the industry in the few years since the turn of the millennium.

There are two distinct camps in security, with one being significantly bigger than the other. In the second and third chapters, I introduce the people in security as a necessary framework for the rest of the book. We started back in the mid-1990s with the Hackers and then came the CASEs.

The Hackers came at a time when security departments did not actually exist in the corporate world. In most cases, they were people who worked in IT operations, or they were programmers, and they were motivated to get into security out of a love of IT. There were many actual white hat Hackers in those days that possessed remarkably diverse skill sets, and never really saw any distinction between work and play. Their "private time" was almost the same as their work time. In their private time, they would read IT books and try out new acts of wizardry.

The second wave came as a result of the perceived failings of the first wave. The first wave of security pros was purely technical and became physically ill when corporate business drivers were discussed. The second wave was more "mature," took the International Information Systems Security Certification Consortium Certified Information Systems Security Professional [(ISC)^2 CISSP] exam, "looked the part" (they wore shirts and neckties), sounded the part (they used buzzwords), and was more aesthetically pleasing to senior management. But the second wave took on a pale complexion and started sweating at the mention of terms such as TCP/IP or "false positive."

One factor stayed common through these formative years in security up until today: *senior managers were never well advised in security.*

The major theme of *Security De-Engineering* is how most of our problems today are borne from a distancing of security professionals from the bits-n-bytes.

The changing of the guard in security from the Hackers to the CASEs has led to a variety of other problems, but the root of all these problems is a certain disconnect—a disconnect between risk management and the information on hard disks, tapes, clouds, and so on. In Chapter 4, I discuss in detail how security has changed for the worse.

Automated Vulnerability Scanners

One of the most detrimental developments in the early 2000s was the widespread acceptance of the automated vulnerability scanner (or "autoscanner" as I will refer to it here). Autoscanners such as Nessus and GFI LANguard came with a promise of finding your server and application vulnerability with the touch of a button; all you need to do is "spend a few minutes" checking for false positives.

The autoscanner seemed at first glance to be like a dream come true for the security world. In the eyes of managers, including our managers in TSAP (TSAP is the pseudonym I give for my first employer in security: a global service provider; I was working with TSAP from 1999 to 2004 based in the Asia–Pacific (APAC) regional HQ in Bangkok, Thailand), the nasty person with green hair and expletive-bearing T-shirt (the multitalented and highly skilled IT professional) could be replaced by a fresh graduate.

In Chapter 5, I outline the impact that the rise of the autoscanner has had on risk profiles, and whether or not the Hacker can really be replaced by a lesser skilled (and therefore cheaper) person who can enter

IP addresses in an autoscanner configuration, hit the enter key, and then attach the automatically generated findings report to an email.

How much value do these tools actually bring to information risk management? A discussion on autoscanners is long overdue because they are so widespread. Popular commercial software tools use an autoscanning engine such as Nessus, and they take center stage in most organizations' vulnerability management strategies.

Mammas Don't Let Your Babies Grow Up to Be Security Analysts

People, be they undergrads or other types of IT professional, usually have some fairly grandiose ideas about what a career in information security may be like. Aside from the discussion about IT operation's relationship to security, in Chapter 6, I discuss the picture with careers in security. I attempt to give a picture of the typical consultant or analyst role, and how it fits with the corporate structure. I give some advice to more technically oriented people who are thinking about getting into information security, and I also give some advice to those IT enthusiasts who are currently working in a security department.

Love of Clouds and Incidents

In the year 2000, there were distributed denial of service (DDoS) attacks carried out against Amazon, Yahoo, CNN, and buy.com. During my time with TSAP from 1999 to 2004, there were very few publicly declared incidents.

Several times, clients had asked us to justify why they should spend on our services—a question that sales and management staff struggled to answer. With the aforementioned DDoS incident from 2000, the managers in TSAP were actually happy to hear of this incident. It was not exactly champagne and cigars, but it was almost. The mindset was something like this: "our invoice amounts cannot be justified because there is really no bad stuff happening in the world—but now there is some bad stuff. You see? DoS is real—it actually happens."

As I will explain in Chapter 8, I do not believe the security industry needs to celebrate incidents in order to validate itself. When the security industry became de-engineered through the 2000s, security managers lost all hope of ever being able to convince the C-level executives of the need for investment in security, other than just passing the audit. But the reality is it is quite possible to change this state of affairs for the better, and this does not involve rewriting the books or reinventing the wheel or moving to another planet.

With a reinfusion of *properly managed* tech resource into the information security game, we would never struggle to justify our existence. We could confidently stand in front of whoever asked, look them in the eye, and tell them what was needed in order to efficiently manage risk. Sounds like I have gone mad? That would not be a surprising reaction to me, and I do not blame you.

Another buzzword has recently been added to the nonstandard, noninternational vocabulary of information security words, and that buzzword was *cloud*. Security pros saw the dawn of cloud computing as an opportunity to find new intellectual capital that would be of some value to organizations, and in so doing, they would feel useful and appreciated again, and everyone would live happily ever after.

I receive on average approximately 10 notification emails everyday from forums and so on that relate to cloud security. There are seemingly thousands of "cloud security experts" now. There are terabytes of drivel in blogs on the subject.

With the cloud security showpiece, there are some slightly new security considerations to take into account, but it is not a radical new model to consider. Regardless of the cloud type, the cloud does not symbolize a new dawn for security. There should not be any need for firms to spend exuberantly on the acquisition of specific cloud security skills. Migration to the cloud presents a security challenge that is not too dissimilar from outsourcing IT operations functions or creation of VPN (virtual private network)-linked regional offices.

Taking cloud security as an example, in Chapter 8, I lament on the desperate search for new intellectual capital in security. It should not be necessary for security pros to have to do this because if one were to look in the right places, one would find plenty to learn that is of *real* value for businesses.

On a separate but related theme, there is this idea that has been afloat from the very beginning about an all-knowing, all-seeing organization that gathers incident data and stores them in a database. The idea is that if we can somehow create a database of all security incidents and categorize them, then after some time, we will have a valid source of evidence (of vulnerability to a threat) to show to the decision makers when we go looking for cash. Again, I do not think we need to go looking for incidents in order to validate ourselves. In Chapter 8, I discuss this point and also the practical difficulties associated with gathering incident data.

Security Products

In Chapter 9, I look at some examples of security technologies and consider them in the light of return on investment.

There is an awful lot of zero-day activity in the underworld these days. Undisclosed malware and undisclosed vulnerabilities are rife. If we are in a situation where we are under some sort of zero-day attack, we cannot detect the attack with pattern matching. We need detection technology that can alert us on the basis of generic indicators (I nearly used the term "heuristic" there, but I refrained; that term is heavily abused by some of the security product vendors).

In Chapter 9, I look at network intrusion detection systems (NIDS) and intrusion detection systems in general. I do not question the value that detection has for information risk management, but I do question the value of the technology currently available to us in security.

In Chapter 10, I look at identity management (IdM) and security incident event management (SIEM) solutions. In both cases, I look at some of the factors that can lead to the vendors' marketing promises being broken.

Especially with SIEM, there are many requirements that firms need to fulfill if they are to see some value from their investment. SIEM should only be considered as a technology that supports incident response, and incident response is more about people than technology. Certainly if there is no incident response capability, the purchaser will not see any value from their SIEM solution, perhaps other than a nice network diagnostics tool for IT and network operations team.

Some of the considerations with SIEM are similar to those with NIDS. There is a sizable initial investment, and then there are on-going operational, maintenance, and initial fine-tuning requirements.

Even for large-sized organizations, IdM products are not necessarily economically viable in every scenario. The organization considering an IdM acquisition must understand what they currently have in the way of user management technology, and which users need access to which resources. Application layer protocols for centrally managing user accounts have been around for a long time, plus many applications may not be compatible with the new IdM solution. In Chapter 10, I take a closer look at the IdM picture. Larger organizations will in most cases already have Lightweight Directory Access Protocol or Active Directory. They need to ask themselves exactly what it is that the IdM solution will do for them on top of their existing technologies.

A Period of Consequences

When I was writing this book and thinking about its content and structure, some famous quotes from history came to mind, and I was reminded of a topic that was similar in some ways to *Security De-Engineering*. The subject was global warming, as portrayed by Al Gore in his *An Inconvenient Truth* road show and documentary.

In *An Inconvenient Truth*, Al Gore quotes Winston Churchill in his pre-World War II warning about rising nationalism in Germany: "The era of procrastination, of half-measures, of soothing and baffling expedients, of delays, is coming to its close. In its place we are entering a period of consequences."

Global warming is related to climate, and the premise that humans are causing global warming is a very difficult one to prove definitively. There is warming (maybe), but is it caused by increasing levels of carbon dioxide? Frankly, climate is too complex for anybody to answer this question or even make sensible estimates.

Corporate information security is complex, but not as much as climate. We can make definitive statements about the relative levels of risk, even if we cannot put numbers to it, and we are aware of the threats. We cannot read the future and say for sure what will happen if we ignore the risks, but we can extrapolate and make educated estimates.

Like many other security professionals, I believe that incidents that result in financial losses are becoming more frequent, and the incidents themselves are no longer just a few malware incidents. The incidents such as the January 2010 Google incident will become more frequent mostly because of the worsening financial climate in the world, and quite frankly, even in a "cool" tech giant like Google, the door was proved to be almost wide-open.

The de-engineering of security departments has led to a situation where corporates are wide-open to attack by automated and manual means, either from "outside" or within their own private networks. Just as with pre-war Germany, we are entering a period of consequences.

Some of the consequences of the current de-engineered security world have already emerged, and I am not just talking about the widespread incidents. In some cases, senior managers have lost their patience with security departments and totally disbanded them. The functions of the security team were passed to IT operations. As I explain in the first chapter of this book, do you blame the managers for this? Personally I do not think you can blame the managers.

From what I have seen of the vast majority of organizations, if they are targeted, they are very likely to suffer major financial losses. The corporate world is now at a stage where we need to make a decision. The drivers for most acts of skullduggery these days are economic, and we are still in a very slow, stagnant period of recovery from the worse recession since the 1930s. There are two choices: we either improve the way we handle information security, or we make a phased migration back to using pens, paper, manual typewriters, and filing cabinets. We either act or be acted upon. If we are acted upon, the situation could be disastrous. Businesses have grown used to the efficiencies that IT allows. Bosses were able to cut staff numbers, and the general public was able to avoid queuing in bank branches and use ATMs instead. What happens if all these innovations are suddenly removed overnight? With the more recent buzz of the threat of cyberwarfare, how safe are national infrastructures from attack?

Another thing that is changing fast is the complexity of software. As software gets more complex, it gets more buggy and open to abuse by fiends. There are endless dialogues on how to get software developers writing secure code, but the efforts are like those of a dog chasing its own tail. Software bugs are here to stay, and the motivations for exploiting them also are not going away anytime soon.

Security Reengineering

The title of this book is *Security De-Engineering* in that the major theme is about how today's information risk management practices have become so unbalanced. The juggling act in security is one of balancing too much or too little technical detail in our risk analysis, while also balancing the costs of safeguards against the goals of the business. Now there is an ever-growing need to shift the balance back to a more analytical approach. So how do we do that? After all, in today's social paradigm, a pure discussion of problems is oh so "negative."

In the last chapter of this book, I do talk about solutions, but although my original plan was to talk in some detail about the solutions, I found that the discussion of the problems already took up a lot of real estate. Clearly we need to identify the problems before we can solve them, so the details of the solutions will need to come at a later date. In Section 4 (Chapter 11) of this book, I do give some ideas on the solutions, although some of the answers will be apparent in the discussion of the problem.

I think the main drive of the solution has to come in the propagation of the appropriate skill sets and an associated structure of professional accreditation (in this book, I do not focus much on the accreditation problems we face today—mostly because I think the problems are relatively well known). Security departments will be quite different under this new scheme, and the tools and products in use will be different, but I am not of the opinion that we need to go back to square one and totally reinvent the wheel. Such disruption will not be necessary.

The ideas put forward in this book may be familiar to some readers. Occasionally, when I comment on the state of play in security, I will get a response to the effect that I was not making a point that was new to the reader. I commented in a blog once on Web application testing, and I got a sarcastic response "thanks for giving us the status quo." Really though, even if what I have written is well known to some people, I am quite sure that the majority are not at all aware of most of the problems, and if they are, nobody has ever hammered out a description of the problems in black and white.

In any case, it is clear that the decision makers and C-level executives are not aware of the problems, and we, as security professionals, have to make them aware. Right now, they probably will not listen to us (and I do not blame them), but I believe the drivers for change in our industry are coming soon. They will most likely come from new regulations and then auditors. How we change is important. Businesses cannot afford to change just for change's sake.

In the best case, what you are about to read is something you have known for a long time, but are not willing to admit the truth to the senior managers above you in the food chain. But for the sake of everyone's principles and, ultimately, at the end of the day, their sanity, it is time for us to come clean with the decision makers and budget signatories.

With *Security De-Engineering*, I hope to be able to get us on the same page in terms of problems. Just talking about problems is not cynical or nonconstructive in this case. It is the first step to solving the problems—and that is not nonconstructive, even if it is a double negative.

The book is clearly not intended to be a technical manual or tutorial; in fact, it is very far from that. I aim to talk about principles and ideas that are not too high up in the clouds to be discussed at the senior management level. Some of the content in this narrative is too detailed for senior management (rather, I should say that senior managers' time is too valuable to be spent listening to too much detail), but then there are also plenty of ideas that should be acceptable as advisories in themselves, or at least serve to illustrate an advisory.

I also do not talk about the better-known aspects such as malware and employee awareness schemes, or "how long should a password be?" These are areas that the industry deals with in a standard way, and they are well covered. Anyway, I only talk about problems that I believe can be solved. The problems such as malware and awareness will never go away for quite some time to come, and it seems to make more sense to take the approach "we will get malware problems and other issues resulting from Homo sapiens doing stupid stuff," and then plan for this to happen.

Information security is not the coolest, most enjoyable, most rewarding, or the most prestigious area of vocational IT today, but it should be and it can be. And when we are back at that point when security is a fun place to work again, business will be spending better, and although it may not be obvious to you at this time, the two are connected. There will of course still be problems. Nobody can promise that there will never be any more financial losses from incidents, but there will be a high level of trust that senior management has in their information risk management strategy and the people who carry it out. Doesn't that sound better?

Even if we cannot address any of our problems in our lifetimes, at least I hope you can learn something from this book. If nothing else, I hope you enjoy reading *Security De-Engineering*.

Author

Ian Tibble was an IT specialist with IBM Global Services before entering into the security arena. His experience of more than 11 years in information security allowed him to gain practical risk management expertise from both an architectural IT and a business analysis aspect. His experience in Infosec has been with service providers Trusecure (now Verizon) and PricewaterhouseCoopers, and also with end users in logistics, banking, and insurance. He has been engaged with security service delivery projects with close to 100 Fortune 500 companies and multinational financial institutions in Asia (Indonesia, Singapore, Malaysia, Taiwan, Hong Kong, and Australia) and Europe.

Contents

Section 3 Security Products

Section 4 The Re-Engineering of Security