SCRAPPY INFORMATION SECURITY™

The Easy Way to Keep the CyberWolves at Bay

SCRAPPY ABOUT

MICHAEL SEESE

“Scrappy Information Security” Book Excerpt

By Michael Seese
Foreword by Craig T. Johnson, M.A., Lead Professor, Capitol College, Information Assurance Master's Program

A Happy About® series
20660 Stevens Creek Blvd., Suite 210,
Cupertino, CA 95014

BOOK EXCERPT Table of Contents

Contents

NOTE: This is the Table of Contents (TOC) from the book for your reference. The eBook TOC (below) differs in page count from the tradebook TOC.

Foreword by Craig T. Johnson

As one of our industry's icons, Mr. Chuck Easttom stated in a foreword to his text on Network Defense that the hottest topic in the information technology industry today is computer security. Moreover, one of society's major challenges is to educate the public about computers, since uninformed users often are intimidated by technology. That lack of knowledge is the first vulnerability in the security of all computer systems. "Not knowing" has another description often perceived as derogatory: ignorance. Yet, ignorance literally means the state of being uninformed, not knowing, or lacking knowledge. Infants entering the world are innocent human beings lacking knowledge. They are ignorant of knowledge, and the duty of those serving as guardians to them is to pass on the knowledge that they need to recognize dangers, and operate autonomously, responsibly, and independently. So, the notion of ignorance is not derogatory because we all suffer from some form of ignorance. The unfavorable aspect of ignorance is the desire to remain in a state of ignorance by choice. Michael Seese is seizing the opportunity with this book to educate others about information security.

When Michael took my class at Capitol College in 2002, we engaged in a journey to bring the principles of security and information technology together, to validate that the two disciplines were not mutually exclusive. The two entities must be

joined as one to allow one to complement the other. Many in that class, much like Michael, have gone forward in their careers and have made significant contributions in their respective fields.

This literary effort by Mr. Seese is important because the work brings the basic principles of information security to the level that a novice can understand. But this book is much better than a typical "how-to" book. Several passages ask provocative questions which will resonate with the average person. Readers will not be intimidated by the jargon typically spoken by practitioners that often have people running to the doors to leave the area, or falling asleep due to boredom. Michael's easy writing style places readers in the correct receiving mode to understand information and concepts. Telling little stories in the book is a nice touch that Michael uses to provide an understanding of specific principles, applications, and topics about information security.

This book will be well received by those novices whose eyes roll back in their heads when hearing the terms "firewalls," "cyber-security," "access control authentication," "non-repudiation," "intrusion-detection systems," or "security-in-depth." End users of computers will want to have this book nearby for the practical knowledge, hands-on advice, and correct steps to take during certain situations. Enjoy the read.

Cheers!

Craig T. Johnson, M.A.
Lead Professor,
Capitol College Information Assurance Master's Program
Doctoral Candidate

Preface

"Be afraid. Be very afraid."
- *Yakko Warner*

Sciences such as engineering, physics, and medicine have been around for centuries. Even so, these disciplines still see advances in their body of knowledge every day. But the modern growth at least has had an established foundation to build upon. In contrast, information security—indeed, IT as a whole—is an immature industry, comparatively, still in diapers. The early computers—mainframes—had built-in security in that they were huge (I've never heard of a mainframe being stolen out of the trunk of someone's car), they were not networked outside of the organization (or even ***in*** the organization!), and only super-smart geeks could run them anyway.

Then the PC happened.

Then the LAN card happened.

Then Al Gore happened.

Then the Internet happened.

And then, e-commerce happened.

The Information Age was fully upon us, and suddenly, every worker was a knowledge worker and every consumer an e-shopper. For a few glorious moments it seemed that a whole new world of possibilities was opening up for humankind.

Then the trouble began.

chapter

1 InfoSec 101 – Definitely *Not* for Dummies

"The user's going to pick dancing pigs over security every time."
- *Bruce Schneier*

You have to learn to crawl before you can walk. It's no different when learning about information security. But your first baby steps probably should not include thumbing through some of the tomes out there with upwards of 500 pages. And you sure don't want to start with something like one book I came across, the "sumo wrestler" of security books, with over 800 pages and weighing in at over three pounds. Let us assume that you have a life, and don't want to spend it flipping through such a text until you are well into your nineties. Instead, let us start with the essentials, shall we?

When teaching "InfoSec 101," I reflect back on my early career as a reporter, and focus on answering the standard questions: who, what, why, where, when, and how. Since this is a Scrappy Book, let's throw caution to the wind and take them out of order:

Why Do We Need InfoSec?

Because our stuff is valuable. Sure, it's mostly invisible stuff, but so are integrity, justice, and love. Back when we made valuable stuff we could see, we locked the stuff up. Information? That simply supported the business. Today, information often *is* the business. In some sense, the challenge we face today is in the lack of "stuff." My paycheck isn't "real" money. It is information transferred from my employer's bank account to mine. My 401K, which recently became a 201K in the stock market tumble, is just numbers in a book. The virtual world is becoming more "real" every day. There are new, profitable companies that provide virtual pets, and then charge customers to purchase, maintain, and "feed" them. And, the lines are blurring: I can use real cash to buy e-money for my avatar so that he can function in his world. But he never sends anything back….

But how do I know if something "un-real" has been stolen? An even more unsettling question—how do I know if something un-real has been altered, or just copied without taking it?

Who?

Everybody.

A chain is only as strong as its weakest link. So everybody has to be a pillar of infosec strength! Executive management must enthusiastically support and adequately fund a security program. The tech guys must do their propeller-head things, such as implementing so-called foolproof technical controls wherever possible so that the majority of us simply cannot screw up. And last, but really *really* certainly not least, every single one of those gosh-darned end users must understand the threats, stop their running-with-scissors behavior, and implement good security practices that they maintain day after day. As technological solutions improve, the bad guys will increase their attacks on the user community. There are a number of reasons for upping the attack rate, but the simplest is this: just as Willie Sutton said that he robbed banks because "that's where the money is," attackers will go after end users because that's where the valuable information is. And even if the criminal element were not actively trolling for unsuspecting knowledge

workers, consider that a 2009 report from the Identity Theft Resource Center said that there were 656 data breaches reported in 2008, up from 446 in 2007, with human error accounting for 35%, the largest single cause.[1]

What?

We've all heard of the "elevator speech:" explaining something in the time it takes an elevator to travel from the ground floor to the top of a reasonably tall building. For an information security professional, the elevator speech can be distilled down to three letters: the "CIA triad." No, it's not some dark reference to a black-on-black clandestine operation. It is a vain attempt to make infosec sound exotic and fascinating. The components are:

- *Confidentiality:* The assurance that information remains "secret," or not accessible to those who should not see it, which usually includes most of the 1.5 billion people with Internet access.
- *Integrity:* The assurance that information has not been tampered with by any of those multi-billion peeps.
- *Availability:* The assurance that information and/or systems can be accessed at all times, a criterion that pretty much guarantees that the first two criteria are almost impossible to meet with absolute certainty.

Where?

Everywhere we possibly can, which often is referred to as "defense in depth," or DiD. The analogy used for years by information security professionals was that of a castle, surrounded by a deep moat and protected by thick stone walls. A less powerful, but tastier, metaphor is, "The crunchy shell around the soft, chewy center." This logic is easily

1. Downloaded 1/7/2009 from http://tinyurl.com/8f9lj8 washingtonpost.com/wp-dyn/content/article/2009/01/05/AR2009010503046.html?wpisrc=newsletter

understood since it applies outside of the infoworld. In the real world we build fences around the compound, hire guards, and put locks on the doors. In the infoworld, we use logical access controls: PC login credentials, network login credentials, file access controls, and role-based access. But the game is changing. The virtual perimeter of our information compound is expanding. We are allowing our business partners and customers to access (hopefully different) portions of our systems. And laptops, standard issue for many employees, somehow are lost, stolen, or simply left unattended and vulnerable. The encrypted communication of a virtual private network (theoretically) ensures that a secure tunnel manages to traverse the wilds of the Internet without compromise. But many organizations are finding that they cannot hold back the world of wireless, which allows the first leg of the connection to be made not from the (also theoretically) secure, wired confines of their home office or a hotel room, but through the air. Any traveler who has accessed his email by "borrowing" the unsecured wireless network of a nearby business or residence can imagine how big of a headache this causes your typical infosec guy.

When?

The simple answer is always: 24 hours a day, 7 days a week, 365 days a year. The threats never sleep, and neither can the protection. Keeping information secure at work is comparably easy. Refraining from discussing potentially sensitive topics in a public place, or making sure your airplane seatmates in economy don't peek at your documents, is harder. Ensuring the security of any information—be it personal or corporate data—on the same PC that an employee's child uses to play online games and surf to any and every site which strikes his fancy is impossible.

How?

"Impossible" problems call for creative and innovative solutions. A winning combination consists of physical, technical, and administrative (PTA – easy to remember if you've ever had a kid in school) mechanisms:

- *Physical:* locks, guards, doors, badges, alarms.
- *Technical:* hardware, software, network architecture, host hardening.
- *Administrative:* policies, passwords, file access control.

We'll address common technical, physical, and administrative security techniques, some of which are fascinating only to those pasty-faced IT workers who haven't been out in the sun for a decade. But an effective information security program, and especially the effectiveness of administrative controls, requires that every person with access to your system be educated about the risks, and his or her responsibility for protecting critical information. Imagine how thrilled your busy colleagues will be to find themselves invited to attend a training session on information security! And I'm sure you will be equally enthused about standing in front of a room full of captives for hours at a time….

Clearly, some of the topics—such as safe surfing and strong passwords—are both critical to your organization's mission *and* applicable to your employees' lives outside of the corporate walls. As such, employees will probably be at least mildly interested in learning about these concepts. Other topics—such as how the Internet works—might be a harder sell since it's not necessarily connected to their professional or personal lives. After all, since you don't need to know how the internal combustion engine works to drive a car, not many people take the time to learn about that either. Still, I would be willing to bet that most folks would be at least somewhat curious about exactly how an email message gets from one person to another. Because a better understanding of this process can improve someone's appreciation of the challenges of information security, I believe that this concept is worth discussing in a training session. Of all the topics covered on subsequent pages, I would say my baker's dozen

of the coolest and most important ones—the ones that the average modern human will care about, or at least find somewhat interesting—are:

- Packets, headers, ports & MACs
- Routers & bridges
- Firewalls
- Encryption
- Access cards
- Biometrics
- Email/spam
- Malware
- Passwords
- Safe surfing
- Wireless
- Laptop security
- Social engineering

Statistics on learning and forgetting are not encouraging, and the likelihood of compliance is discouraging enough when people *do* remember what they have learned. In the late 1800s, German philosopher Hermann Ebbinghaus found that more than 50% of random items learned were forgotten in less than a day. After one month, more than 80% were forgotten.[2] If your training is going to achieve anything more than checking off a requirement on your implementation plan, you're going to have to find ways to make this information stick, and then inspire people to go out and apply what they learn with the discipline of a Kung Fu master. A talking head at the front of the room gesturing lamely at a bunch of crowded PowerPoint slides just isn't going to cut it.

---

2. Downloaded 3/12/2009 from http://encarta.msn.com/media_461547609_761578303_-1_1/forgetting_curve.html

The chapter on training is chock full of tips to enable your training to get results. However no amount of training in the world will make up for flimsy technical designs or amateurish physical protection, so let's get busy on physical and technical security first.

About the Author

Michael Seese, CISSP, CIPP, is an information security, privacy, and business contingency professional in beautiful Chagrin Falls, Ohio. He holds a Master of Science in information security, which was earned completely online via a very cool synchronous and interactive curriculum, and a Master of Arts in psychology, which tends to scare people. He began his career as a journalist, and then moved into technical writing, which piqued an interest in programming, which after all is nothing more than another form of writing, using a more limited and concise language. Then one day, standing in a local bookstore and surrounded on three sides by programming books, covering C++ and C-sharp and .NET and ASP, he had an epiphany: programming languages come and go. Guess wrong—that is, specialize in the flavor-of-the-last-month—and some college fresh-out will take your job, and probably do it

better. But the need to store data and protect data will remain and, in fact, grow. That realization led to his current career track.

Michael regularly speaks at conferences, has had numerous articles published in professional journals, and contributed two chapters to the 2008 *PSI Handbook Of Business Security.* He is the co-author of *Haunting Valley*, a compilation of ghost stories from the Chagrin Valley. Michael also penned (or, better said, e-penned) the twin books *Scrappy Information Security* and *Scrappy Business Contingency Planning*. He currently spends his limited spare time rasslin' with three young'uns, and can be reached between matches at scrappy@MichaelSeese.com.

Getting "Scrappy Information Security" (http://happyabout.info/scrappy-infosec.php)

"Scrappy Information Security " can be purchased as an eBook for $14.95 or tradebook for $19.95 at: http://happyabout.info/scrappy-infosec.php or at other online and physical book stores.

Please contact us for quantity discounts sales@happyabout.info or to be informed about upcoming titles bookupdate@happyabout.info or phone (408-257-3000).

Happy About is interested in you if you are an author who would like to submit a non-fiction book proposal or a corporation that would like to have a book written for you. Please contact us by e-mail editorial@happyabout.info or phone (1-408-257-3000).

Other Happy About books available include:

- Scrappy Project Management®: http://happyabout.info/scrappyabout/project-management.php
- The Business Rule Revolution: http://www.happyabout.info/business-rule-revolution.php
- Climbing the Ladder of Business Intelligence: http://www.happyabout.info/climbing-ladder.php
- Offshoring Secrets: http://happyabout.info/offshoring-secrets.php
- Overcoming Inventoritis: http://www.happyabout.info/overcoming-inventoritis.php
- Collaboration 2.0: http://happyabout.info/collaboration2.0.php
- 42 Rules for Successful Collaboration: http://www.happyabout.info/42rules/successful-collaboration.php
- I've Got a Domain Name—Now What???: http://www.happyabout.info/ivegotadomainname.php
- I'm on Facebook—Now What???: http://happyabout.info/facebook.php
- I'm on LinkedIn—Now What???: http://happyabout.info/linkedinhelp.php
- Twitter Means Business: http://happyabout.info/twitter/tweet2success.php
- The Successful Introvert: http://happyabout.info/thesuccessfulintrovert.php
- Blitz the Ladder: http://www.happyabout.info/blitz.php