CYBER SECURITY

Rules to Live By

Ken Buckler

Cyber Security: Rules to Live By

Ken Buckler

This book is for sale at http://leanpub.com/cybersecrules

This version was published on 2021-12-12

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Also By Ken Buckler

Death by Identity Theft

Building Greatness

Hagerstown: The Hub City Adventure Guide

Hacking of the Free

Surviving Uncertainty

For my faithful dog, Legend, who crossed the Rainbow Bridge in 2021.

Contents

About the Author

A Cyber Security Professional with Over Ten Years of Experience

Specializing in Cyber Security Analytics and Risk Management, Ken has provided services to commercial and Federal clients. He has analyzed the cyber security posture of large distributed enterprises of over half a million computer systems, including vulnerability and threat applicability and analysis.

Ken holds a Bachelor's Degree in Computer Science from Mount Saint Mary's University as well as CompTIA Security+ and CompTIA Advanced Security Practitioner certifications.

Read more about Ken at www.KenBuckler.com

Legal

The author and publisher have strived to be as accurate and complete as possible in the creation of this report, notwithstanding the fact that he does not warrant or represent at any time that the contents within are accurate due to the rapidly changing nature of the Internet and the field of Cyber Security.

Although the author and publisher have made every effort to ensure that the information in this book was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause. An attorney and/or cyber security consultant should be contacted in any data breach situation

While all attempts have been made to verify information provided in this publication, the Publisher assumes no responsibility for errors, omissions, or contrary interpretation of the subject matter herein. Any perceived slights of specific persons, peoples, or organizations are unintentional.

In practical advice books, like anything else in life, there are no guarantees of income made. Readers are cautioned to reply on their own judgment about their individual circumstances to act accordingly.

This book is not intended for use as a source of legal, business, accounting or financial advice. All readers are advised to seek services of competent professionals in legal, business, accounting, and finance field.

This book does not reflect the opinions or views of my employer or clients. All mentions of vendors, companies, or software products are registered trademarks of their respective owners, and are not endorsements or reviews, and provided for educational purposes only.

Introduction

My first computer was a VIC-20 in the late 1980's. Funny thing about that computer, it was actually only one year older than I was. The VIC-20 was top-of-the-line for its time, with a whopping 5KB of RAM, expandable to up to 32KB. Programs and data could be stored using an audio casette drive, or if you could afford it, a 5 1/4 inch floppy drive. The VIC-20 didn't have an operating system, and everything had to either be typed in by hand, loaded from a casette tape, or loaded from a ROM cartridge similar to 80's and 80's gaming consoles.

All of the programs for the VIC-20 were written in the BASIC programming language. Memory was accessed through "PEEK" and "POKE" commands. The most interesting part about "POKE" commands is that access to memory was for the most part unrestricted, allowing the user to "hack into" any program in memory, cheat at games, or even potentially crash the program. Looking back, I wonder if the early designers of this system understood the potential problems which would eventually be introduced by giving the user direct access to memory. While the risk was extremely low in single-user, standalone environments, as computers evolved into networked, multi-user systems, the direct access of memory by the users and their applications has resulted in numerous security vulnerabilities such as buffer overflow or buffer underrun.

Much of the history of computing and the internet was originally viewed as being only for academic or government usage, with all users trusted to "behave" and not attempt to maliciously use or interrupt the system. Even modern-day communication protocols such as TCP/IP and UDP are inherintly insecure, originally designed to only be used in a "trusted" environment, and must be augmented with additional "secure" protocols layered on top of the base protocols. If you're not a very technical person, these last two paragraphs have probably sounded like jibberish to you, and that's okay. It is my intention to write this book from the simplest perspective possible, using analogies where I can to help less technical readers better understand fundamental Cyber Security concepts.

"Be Prepared" was probably one of the most important lessons I learned in Boy Scouts. Infact, I would say it probably has been a driving force in my continuing efforts to always improve security procedures and policies.

After publishing "Death by Identity Theft", I wanted a book which could be used as an introductory primer to Cyber Security. Originally this book was going to be published in early 2020. As they say, "no plan survives first contact with implementation." I had to put this book on hold due to ever-growing concerns about election hacking and social engineering being used to influence our elections in the United States. So, "Hacking of the Free" was born, and this book remained untouched.

As I finished writing "Hacking of the Free" the entire world was turned upside down by a global pandemic. These were scary times for many of us. Supply chain interruptions caused shortages at local grocery stores of many essential goods. Of course, as a cyber security professional I try

to plan for every contingency. I spent the year preparing in case things got really bad, including acquiring (and growing) extra food and other supplies in case supply chain issues worsened with a large outbreak increase. Fortunately, the contingency I planned for never happened.

As the COVID-19 pandemic was starting to come to a close through the distribution of vaccines and the reopening of businesses, finally I was able to pick back up my work on this book. Much like the supply chain contingencies I planned for but never experienced, much of Cyber Security is not only trying to prevent adverse events from happening, but also planning for those events which may never happen, such as a malware infections, natural disasters, or complete physical hardware failures. Periodic reviews of response plans must be carefully performed, and plans revised as needed to address previously unforseen contingencies. Now I, like many other people around the world, will probably always have a year's supply of toilet paper "just in case." And that's really not such a bad thing, to be prepared.

Ironically, while real-world supply chain issues were occuring, another supply chain issue was secretly happening behind the scenes. In what was most likely a foreign nation state attack, the server monitoring software SolarWinds was compromised with malware. For many organizations this was a worst case scenario which many had never planned for - a comprimse of not only a software vendor, but compromise of security monitoring software. Within hours of notification from SolarWinds, organizations had to completely shut down all SolarWinds monitoring servers and begin the painstaking process of performing forensics on every server, and their entire Active Directory domain, due to the potential for complete network compromise. The impact on the entire industry is only starting to be realized, as many organizations now need to re-think their approach to security to include additional redendancies.

This is not an all-encompasing guide to everything you need to know about cyber security. Information technology and cyber security are an ever evolving field, and as such no single book can ever teach you everything you need to know. Think of this book more as a primer - an introduction to important concepts which should be further explored and understood. Much like many organizations are realizing after the SolarWinds compromise, Cyber Security is an ever evolving field, and no matter how much planning, how much studying, and how much research you do - you'll never be able to plan for everything.

Chapter 1 - Even The Unsinkable Titanic Sunk

July 29th, 1908 - The design for a new ship, the RMS Titanic, is approved.

March 31st, 1909 - The keel of the RMS Titanic is laid.

May 31st, 1911 - The hull of the RMS Titanic is launched.

March 31st, 1912 - The RMS Titanic is considered “completed”.

April 2nd, 1912 - The RMS Titanic begins sea trials.

April 10th, 1912 - The RMS Titanic departs on her maiden voyage across the Atlantic Ocean.

April 14th, 1912 - The RMS Titanic strikes an iceberg.

April 15th, 1912 - The RMS Titanic comes to rest on the bottom of the Atlantic Ocean.

After twenty six months of construction and a week of sea trials, the RMS Titanic set sail on its maiden voyage across the Atlantic Ocean. The Titanic’s double-plated bottom, as well as sixteen watertight compartments designed to prevent flooding from spreading in the case of a hull breach, were designed to make the ship practically unsinkable.

And yet, just a few days later on April 14th, the Titanic would collide with an iceberg and begin to sink. While the ship was designed to remain afloat in the case of a head-on collision, designers did not take into account the possibility of multiple watertight compartments being breached simultaneously. Ironically, the crew of the Titanic’s efforts to avoid a head-on collision with an iceberg ultimately contributed to the ship’s sinking.

Walter Lord, author of “A Night to Remember”, put it best. “The appearance of safety was mistaken for safety itself.”

Unfortunately only sixteen lifeboats were aboard the Titanic, less than half what would be needed to safely evacuate the entire ship. Why were there so few lifeboats? Was it because of cost? Was it because there wasn’t enough room on the ship? No, the reason there were not enough lifeboats is that the White Star Line wanted the Titanic to have a wide deck with uninterrupted views of the sea. The White Star Line believed that lifeboats would be used to ferry passengers to a nearby ship in case of an emergency, and never imagined a scenario where all passengers would need to be evacuated without a nearby ship to take them on board.

The Titanic isn’t just the story of an “unsinkable” ship, but the story of multiple systemic failures resulting in complete disaster.

There is no such thing as an unhackable system

Much like there is no such thing as an unsinkable ship, there is also no such thing as an unhackable system.

Perhaps the most “secure” system would be one that is air-gapped - that is, a system which does not have any network connection whatsoever. Even then, this system is still vulnerable to physical attacks, theft, or in even some cases, radio frequencies being used to spy on the computer system remotely, and even influence its behavior.

Cyber Security is not about creating an unhackable system. Cyber Security is about reducing the risk that a system will be breached (confidentiality), modified (integrity), or disrupted (availability) without authorization. These three concepts, confidentiality, integrity, and availability, make up the core foundations of any cyber security program.

Confidentiality - Is the data protected from disclosure to unauthorized users?

Integrity - Is the data protected from modification by unauthorized users?

Availability - Is the data accessible by authorized users for review or modification?

All too often, the third concept, availability, is overlooked or ignored when planning a secure system. While confidentiality and integrity of data are important, that data is useless if it is not available to authorized users.

You don’t need five deadbolts if your neighbor hides his key under the welcome mat

In many cases, cyber security isn’t always about designing the most secure systems possible. In fact, often times cyber security is more about your security being a better deterrent to would-be attackers than your neighbor’s security.

Cyber security should always be a delicate balance of lowering or mitigating risk while maintaining cost effectiveness. If the cost of mitigating a risk exceeds the cost of the impact if the risk event occurs, then from a cost basis that mitigation should not be implemented. However, it’s important to realize that some risk financial impacts are more difficult to measure, for example, the public image impact for a financial institute losing the identities of their customers will far exceed just cleanup and identity monitoring costs, but potentially impact the institute’s revenue for years.

Key Concepts to Know:

Vulnerability - A flaw in a design, a possible means of compromising confidentiality, integrity, or availability

Threat - An external or internal force, either man-made or natural

Risk - The probability of a threat successfully attacking a vulnerability

Typically during the summer months, police departments will put out notices to communities to lock the doors on their automobiles and homes. Similar warnings are often provided in public parking lots, and at events. “Lock your doors!” is repeated over and over. At cursory glance, locking your doors seems futile, especially when a quick hit with a hammer will shatter any automobile or home glass. And yet, locking your doors is very effective in preventing burglary or theft. Why? Because some of your neighbors don’t listen, and therefore have a higher risk of being a victim of a crime. The unfortunate truth is, unless you’re carrying a large amount of cash, or have military secrets stored inside your home or vehicle, the average person simply isn’t worth the additional time it takes to defeat simple security measures to gain access to your automobile or home.

Cyber Security is the same way. Depending upon the sensitivity of the data, you just need to be more secure than your neighbors, and for the most part attackers will leave you alone. For security measures to be successful, the security measures must cost less than the predicted loss, should confidentiality, integrity, or availability be compromised, while making an attacker’s opportunity cost of defeating those security measures higher than the value of a successful compromise.

Note that predicted loss costs of confidentiality, integrity, and availability are calculated separately. For example, the predicted loss cost of confidentiality of financial information, such as a credit card number, is most likely much higher than the predicted loss cost of the availability of that same financial information. As such, the security costs associated with each of these measures should be calculated separately as well.

More simply put, Cyber Security is in essence a cost-reduction strategy used to plan for adverse events. The cost of implementing a cyber security measure should never exceed the potential cost of the adverse event that cyber security measure is intended to prevent.

Chapter 2 - K.I.S.S. - Keep It Secure Stupid!

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Never overestimate the technical ability of the common user

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Never underestimate the technical ability of the common user

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Never underestimate the technical ability of the your attackers

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Common Attacker

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Uncommon Attacker

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Internet is a Dangerous Place

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Ransomware

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Spyware and Adware

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Keyloggers

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Viruses

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Trojan Horses

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Chapter 3 - Never Use a Cannon to Kill a Mosquito

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Cyber Security is about managing risk

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Security is Worthless if no work can be performed

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Is It Safe To Download Computer Software From The Internet

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Intrusion Detection

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

What is an Intrusion Detection System?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Who is Breaking Into Your System?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How Do Intruders Break into Your System?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How Does One Stop Intrusions?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Firewalls and You

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Anti-virus Software

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Who are the Players in the Anti-virus Industry?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Anti-Spyware Software

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Chapter 4 - Trust No One

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

In God We Trust, All Others We Verify - Phishing Explained

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Understanding Phishing

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

What are the Consequences?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How Spammers and Phishers Get Your Email Address

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Top 5 Myths About Phishing

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Don’t Fall for the Bait

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Anti-Phishing Software

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

What's in a Password?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Moving Beyond Passwords: Two Factor Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Chapter 5 - Keep a Secret, Secret

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Passing a Note in Class

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Secret Decoder Ring

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Beyond Encoding - Encryption

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Symmetric Encryption

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Asymmetric Encryption

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Privacy Online

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How do people get this basic information about you?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How do you stop this from happening?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How do I get an anonymous proxy server?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Does an anonymous proxy server or VPN make you 100% safe?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

What other things should I be concerned about when trying to keep my private information private?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Chapter 6 - Two is One and One is None

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Importance of Backups

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Protection You Can Afford

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Importance of Securing Backups

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Importance of Testing Restoration of Backups

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Chapter 7 - Always Take Out the Trash

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

The Internet is Forever

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Delete Does Not Delete

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Recovering Data

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Permanently Deleting or Destroying Data

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

What is Identity Theft?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Types of Identity Theft

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

It Can Affect Anyone

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Not As Difficult As You Think

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Dumpster Diving, Dumpster Fire

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Dumpster Diving

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Mail Stealing

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Shoulder Surfing

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

ATM Skimming

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Check Fraud

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Telephone Service Fraud

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Telephone Scams

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Credit Card Theft

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Phishing

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Preventing Identity Theft

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Protecting Your Mail

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Safeguard Your PIN and ATM/Credit Card

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Protect Your Personal Information

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Avoiding a Phishing Scam

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Additional Preventative Measures

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

When (not if) Identity Theft Happens to You

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Steps to Take in Recovering Your Identity and Line of Credit

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Your Liability as a Victim of Identity Theft

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Actual Identity Theft Victim Cases

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

How Will You be Affected?

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Credit Card Liability

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

ATM and Debit Card Liability

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Check Liability

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

It's Your Responsibility

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Liability Agreements

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Identity Theft Resources

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

Conclusion - A Few Final Rules to Live By

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.

References and Further Reading

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/cybersecrules.