PRAISE FOR
CYBERCRISIS

"***CYBERCRISIS*** will wake you up from a nightmare you didn't even know you were in. Once again, William Keiper has written a book that shines a light for the rest of us."

~Steve Chandler, author of *Time Warrior*

"***CYBERCRISIS*** answers the question, 'How can we harness the value of internet technology without opening the door to our real-lives?'"

~Stephen McGhee, Transformational Leadership Coach and author of *Climb to Freedom* and *Get Real*

CYBERCRISIS

IT'S PERSONAL NOW

CYBERCRISIS

IT'S PERSONAL NOW

WILLIAM KEIPER

FirstGlobal® Partners LLC
dba FirstGlobal® Publishing

Contact the publisher: www.firstglobalpartners.com
Contact the author: www.williamkeiper.com

Chris Nelson, editor
David Moratto, interior and cover design
Alex Cyrell, creative consultant
Selim Aksan, cover photograph (iStock by Getty Images)
Tracy Rasinski, author photo

The material provided herein is for general information and educational purposes only. Although the publisher and author use reasonable efforts to include accurate and up-to-date information herein, no warranties or representations of any kind as to accuracy, currency, or completeness are made. Because of the dynamic nature of the internet, any Web addresses or links contained in this book may have changed since publication and may no longer be valid.

This book is sold with the understanding that the publisher and author do not intend and are not engaged in rendering psychiatric or psychological, medical, legal, or other advice requiring licensure or certification. The information contained herein may not apply to all situations and may not reflect the most current situation.

Rather than use a trademark symbol with every usage of a trademarked name, such names are used only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement, confusion or ambiguity as to ownership. All marks are the property of their respective companies.

Library of Congress Control Number: 2016958606
ISBN-10: 0-9913835-0-8 and ISBN-13: 978-0-9913835-0-4
ISBN-10: 098498934X and ISBN-13: 978-0-9849893-4-8 electronic

For inspiration and support in the creation,
execution and completion of
CYBERCRISIS—It's Personal Now:

Chris Nelson, Jim Manton, Stephen McGhee,
Alex Cyrell, Steve Chandler, Jeff Holtmeier,
David Moratto, Mary Aiken, Ph.D.,
and my wife, Pamala Plummer-Wright.

CONTENTS

INTRODUCTION

THE WEB IS US, WE ARE THE WEB

Click-by-click you are being pulled more deeply into the personalized slice of cyberspace you have created and shaped through your choices.

Each click holds the promise of enhancing your life through immediate access to unlimited online resources of every kind. Each click can expand your social interactions and increase your visibility, far and wide if you choose. Each click also has the potential for sending you into the den of a bad actor wanting to take your money, or with an even darker purpose.

The distinction that has been drawn between "real-life" and "online life," is fading to the point where it's hard to see. However, your online activities often expose you to threats, risks, and consequences in contexts that are quite different from real-life. The patterns you quickly recognize from your accumulation of real-life experiences, often don't translate well enough or fast enough to be of value in your online world.

The principal objective of *CYBERCRISIS* - *It's Personal Now* is to heighten your awareness of some of the factors and conditions that could, in the blink of any eye, suck you into a personal cybercrisis. It represents a warning shot for those of you predisposed to trust your fellow man in the real-world and, without thinking, carry that bias into cyberspace.

Behaviors held in check in the real-world may be readily pursued online. Some of these include voluntarily handing over deeply personal information to strangers, posting a mean, anonymous comment in an online forum, or creating a fake profile as a way of checking up on a spouse or boyfriend.

For purposes of this book, I have assumed that you use a smartphone, email, apps, messaging and social networks, but are not a technology expert. My perspective as the author comes from having been a part of computer technology and software businesses since shortly after the launch of the first Apple and IBM personal computers.

In these public and private technology and related companies, I have served as CEO, board member, and strategic advisor. Through this work, I gained experience, understanding, and perspective, about digital age developments and their personal impacts, good and bad. I have also written two previous books whose driving themes involve greater self-reliance in personal and business life. My hope is that this book will motivate you to accept a higher level of personal responsibility for your digital well-being.

This is not a technical manual about cybersecurity and the most bulletproof ways to protect yourself from Web threats. I do, however, offer some personal cybersafety tips and references in Chapters Nine and Ten. I also provide a Glossary for your reference in understanding terms that may be unfamiliar to you.

Even if you are a technology expert, comfortable with digital technology, or already consider yourself a safe navigator of cyberspace, you may discover some interesting facts and perspectives within these pages.

I chose to keep this book as brief as possible. You should be able to read it in about sixty to ninety minutes. To help speed you along your way, I elected to forego footnotes and other research citations, with a few exceptions. The numbers and other facts stated here are based on data and information I personally researched, and most of which can readily be discovered by keyword or phrase search.

The Web is us, and we as a collective are the Web. After reading *CYBERCRISIS,* my hope is that you will better understand this dynamic relationship, and appreciate the need for self-reliance in cyberspace, just as much as in the real-world.

~William Keiper
www.williamkeiper.com

The illusion is that the cyber environment is safer than real-life —and connecting with other people online somehow carries fewer risks than face-to-face contact ... [However] our instincts, which were honed for the real-world, fail us in cyberspace.

~Mary Aiken, Ph.D., *The Cyber Effect, A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*

ONE
YOU'VE BEEN HACKED

Your personal information will be hacked if it hasn't been already.

When such access has been accomplished, the result is called a data breach; unfortunately, this is a term we know all too well these days. These violations are designed to disrupt the information status quo for economic, political, social and religious reasons. They also are sometimes pursued to gain an advantage in the pursuit of criminal activities or simply for hackers to prove it can be done.

Although the definition of hacking sounds impersonal "Using computers to obtain unauthorized access to data," most significant data breaches sweep up a huge number of individuals.

COLLATERAL DAMAGE

Global enterprises, mid-sized companies, governments around the world, and even the major internet infrastructure companies, face increasingly frequent disruption and the damage associated with data breaches. The impact of hacks on very large-scale information systems is costly and dangerous for the institutions that are targeted, and harmful for their shareholders.

These hacks often become very personal. The Federal Trade Commission has reported that the number one consumer complaint lodged for the past fifteen years running has been identity theft—one significant consequence when vast amounts of personal information are stolen in larger data breaches.

The Yahoo data breach, the largest ever, significantly increased the number of identities publicly exposed this year over last. The following excerpt from an article in *The New York Times* describes how such a massive and seemingly distant data breach—*reported by Yahoo two years after it happened*—can become your problem.

> SAN FRANCISCO—Yahoo announced on Thursday that the account information of at least 500 million users was stolen by hackers two years ago, in the biggest known intrusion of one company's computer network. In a statement, Yahoo said user information—including names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions—was compromised [two years before this article appeared] ... "The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family," said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground Web. "This is one of the biggest breaches of people's privacy and very far reaching."

If you want to know if your personal information was compromised in the Yahoo (or another) data breach, you can go to www.haveibeenpwned.com, a website dedicated to informing victims of data breaches. [Pwned (sounds like owned) is another word for hacked.] Once there, enter your email address, verify that you control it, and a search will be made of Pwned's hundreds of millions of records. As for known breaches, any released information in which your email address has been found, will be reported to you.

"AM I UNDER SURVEILLANCE?"

It's no wonder that Americans have a significant feeling of data insecurity. Pew Internet Research discovered low levels of confidence in the privacy and security of the personal data records maintained by many of the companies and financial institutions with which they do business.

Pew also found that "Americans have a pervasive sense that they are under surveillance when in public and very few feel they have significant control over the data that is collected about them and how it is used."

A few examples from the Pew studies:

- 93% of adults say that being in control of *who* can get information about them is important.
- 90% say that controlling *what* information is collected about them is important.
- Just 9% of adults say they are "very confident," and 29% say they are "somewhat confident," their data will stay private and secure with credit card companies.
- Just 6% of adults say they are "very confident" that government agencies can keep their records private and secure, while another 25% say they are "somewhat confident."

Despite these sentiments, the door to our personal data largely remains open, often through our own negligence. We don't choose options readily available to us that could keep it at least partially closed. (See Chapters Nine and Ten.)

At the level of our own smartphones, tablets, and PCs, we open ourselves to data breaches through the most pervasive of today's communication methods: email and messaging. Symantec produces software for security, storage, and backup, and offers well-researched findings on the subjects. They reported the following on the topic of email:

- For cybercriminals who want to reach the largest number of people electronically, email is still the favored way to do it. It continues to dominate digital communications for both business and consumer use.
- Total worldwide email traffic, including both business and consumer emails, is estimated to grow to over 257 billion emails per *day* by the end of 2020. About half of all inbound email traffic last year was considered spam.

- Email is widely used as the delivery mechanism for spam, phishing, and malware, and all have potentially significant harmful consequences.
- Malware distributed in emails requires social engineering [making the desired action seem familiar and comfortable for the user] to convince its recipient to open the attachment or to click on a link.

Even given their ongoing success using email as a primary delivery vehicle, spammers have now pervasively infiltrated social networking and instant messaging, two of the most-used mobile applications.

DATA FINGERPRINT

McAfee.com, now a part of Intel Security, a provider of security solutions and services, has said that "Data is the 'oil,'" of the digital economy. The oil, specifically, is your personal information when exploited on three fronts. First, your continuous enrollment and participation in social communities so as to drive advertising and other revenues for the platform owners. Second, your personal information when unlocked and made available for purchase by third-parties. And third, the ransoming of your identity or other data crucial for conducting your life.

The core value element in these instances is your personally identifiable information (abbreviated as "PII"). The National Institute of Standards and Technology (NIST) defines PII as:

> "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

I prefer to call this your "data fingerprint" because it is unique, like a fingerprint. This term has been popularized by Terbium Labs, a company that will monitor the Hidden Web (see Chapter Eight) for online mentions of the personal information embodied in your data fingerprint.

The information described in the Yahoo data breach referenced above represents the personal data you regularly offer in an enrollment process with a service provider. At such time, you voluntarily —and probably without much thought—provide a good portion of your complete data fingerprint. Typically, you authorize this by agreeing to the site's terms and conditions: long and complex verbiage you don't read. This information helps those companies monetize your membership through the sale of upgrades and other services, and by selling advertising.

PUBLIC EXPOSURE

The consequences of a personal data breach can include the pain and possible embarrassment caused by the exposure of information expected to remain private. Last year, this became sensationally clear with the public release of the identities of users of the Ashley Madison site. Ashley Madison is an adult dating site that once advertised, "Life is Short, Have an Affair!" Because the purpose of the site was to make it easier for spouses to cheat, people enrolled with the expectation that their personal information would stay private: names, credit card data, physical addresses and sexual preferences.

A group calling itself "The Impact Team" hacked the Ashley Madison site and demanded that it be taken down in protest of certain of the company's business practices, and its encouragement of adultery. With Ashley Madison's ongoing refusal to close the site, the hacked data—encompassing an estimated 32,000,000 user accounts —was released. Individual account details were initially posted to the Dark Web. They were later found to include the names, passwords, addresses, phone numbers and credit card transactions of the site's millions of users.

Very shortly after that, it became a simple matter to enter your spouse's email as an online query on Have I Been Pwned, and other sites, and instantly learn if his or her email address was part of the Ashley Madison data release. You can imagine the conversations that many couples must have had shortly after the news broke of the hack, and then the public release of the records. Although it was a huge breach at the time—just last year—ironically, it no longer makes the Top 10 largest data breaches.

This year a similar organization, known as AdultFriendFinder.com, suffered an even more far-reaching hack. It involved over 412 million user accounts. Over 99% of the user passwords were cracked. Bigger and more popular than Ashley Madison, the hack included email addresses and passwords collected over twenty years. Much like Ashley Madison, however, the details of users who believed their accounts had long ago been deleted, were stolen—in this case for the *second* time in a year.

YOU WILL BE HACKED

Information security is far from bulletproof, and even the best companies, financial institutions, and governments are not able to keep up with technical assaults by hackers. We have witnessed large-scale hacks of major companies leading to the exposure of a total approaching a billion personal identities—*just in the past year.* Corporate record and website data breaches, the release of government files, and intrusions on your own devices, are the vehicles for public exposure of the private information that is your identity.

The more complete the personal information associated with your name, the more credible your data fingerprint, and the easier it is to successfully commit identity theft. A full set of personal information (called "fullz") means a higher potential price should it be made available for sale. (See Chapter 8, The Hidden Web.)

The days when you could expect, and have reasonable confidence, that information about you would remain private, are over. You must proceed on the assumption that who and what you are in private, will one day be examined in the light of day.

There is now and always will be an onslaught of email- and messaging-borne intrusions into your smartphone, apps, and personal data, by unknown assailants. If the past few years are any guide, large data breaches will result in the release of hundreds of millions of full or partial data fingerprints each year.

The Web is important, even essential, to us humans. But it is a highly flawed environment when it comes to ease of exploitation by bad actors. Remember the fighter's admonition: "Protect yourself at all times."

GLOSSARY

ADDICTION A state that is characterized by compulsive drug use or compulsive engagement in rewarding behavior, despite negative consequences.

ADWARE A form of spyware that facilitates the display of unwanted advertisements on a screen.

ANTIVIRUS SOFTWARE Software that is used to detect, delete and/or neutralize computer-based viruses.

BOT Software designed to complete a minor but repetitive task automatically or on command.

BOTNET A collection of compromised computers that is built up then unleashed as a distributed denial of service attack or used to send vast quantities of spam.

BYOD Bring your own device: a business policy of allowing employees to connect to a network from personally-owned mobile devices.

CARDING A term describing the trafficking of credit card, bank account, and other personal information online as well as related fraud services. Carding markets have been defined as full-service commercial entities.

CATFISH Someone who creates a fake profile on a social media platform to seduce people.

COMPULSIVE BEHAVIOR Uncontrolled or reactive behavior.

CRACKING Finding a password by running many combinations of characters.

CRISIS A crucial or decisive point or situation; a turning point. An unstable situation, in political, social, economic or military affairs, especially one involving an impending abrupt change.

CYBER Of, or having to do with, the internet.

CYBERBULLYING The use of the internet to harass, intimidate, or cause harm to another.

CYBERCRIME Any crime that is committed using a computer network or hardware device.

CYBERCRISIS (PERSONAL) Any event or series of events relating to or arising from participation in online activities that has led, or could abruptly lead, to a rising level of personal uncertainty and anxiety.

CYBERPSYCHOLOGIST A person concerned with the psychological effects and implications of computer technologies such as the internet and virtual reality.

CYBERSECURITY The processes and methods of protecting a computer or computer network or information by preventing, detecting and responding to attacks.

CYBERSLACKING A term used to describe the utilization of the internet during work hours for unrelated tasks.

CYBERSPACE The internet as a whole.

CYBERSTALKING The use of electronic communications or tracking technologies to stalk or harass another person.

DARK WEB The portion of the Deep Web that is hosted on restricted networks and not accessible using standard Web browsers.

DATA BREACH A data breach is the intentional or unintentional release of secure information to an untrusted environment.

DEEP WEB The part of the World Wide Web that is not indexed by traditional search engines.

DENIAL OF SERVICE ATTACK In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet.

GIG ECONOMY An economic model in which temporary positions are standard, and organizations contract with independent workers for short-term engagements.

HACK An unauthorized attempt to gain access to an information system.

HACKER An unauthorized user who attempts to or gains access to an information system.

HACKING Use of computers to obtain unauthorized access to data.

HIDDEN WEB The part of the internet that is inaccessible to conventional search engines. Also, known as the *Deep Web*.

IDENTITY THEFT The crime of impersonating someone by using their private information, typically for financial gain.

INTERMITTENT VARIABLE REWARDS Rewards that are handed out inconsistently and occasionally. This usually encourages the person to keep trying or checking until they get what they want, without changing their own behavior.

INTERNET ADDICTIVE BEHAVIOR Compulsive behavior resulting from escalating reliance on internet services or the need to satisfy a craving for internet-related activity. Also called *internet addiction*.

KEYLOGGER A virus, software or hardware that tracks keystrokes and keyboard events to capture private information, passwords or credit card information.

MALWARE Any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising

ONLINE DISINHIBITION EFFECT The loosening (or complete abandonment) of social restrictions and inhibitions that would be present in a face-to-face interaction, during interactions with others on the internet.

ONLINE REPUTATION MANAGEMENT Influencing and control of an individual's or business's reputation. Today, primarily an issue related to search results.

PADLOCK Web browsers typically display a locked padlock icon while using the HTTPS protocol (considered more secure than HTTP). While executing secure transactions on the Web, the submitted information is encrypted using public-key cryptography.

PERSONAL CYBERCRISIS Any event or series of events relating to or arising from participation in online activities that has led, or could abruptly lead, to a rising level of personal uncertainty and anxiety.

PHISHING The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), by masquerading as a trustworthy entity in an electronic communication.

ONLINE PREDATOR People who use the internet to hunt for victims to take advantage of them in any way, including sexually, emotionally, psychologically or financially. They seek to manipulate children and others, creating trust and friendship where none should exist.

RANSOMWARE A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by freezing the user's files unless a ransom is paid.

REAL-LIFE Life outside cyberspace.

REAL-WORLD The physical world, as opposed to the virtual world of the internet.

SCAMMER A person who pursues an online confidence game or other means of deception or fraud, with the objective of a quick payoff for the effort.

SEXTORTION A form of blackmail and sexual exploitation that employs nonphysical forms of coercion by threatening to release sexual images or information to extort sexual favors or money from the victim.

SOCIAL ENGINEERING In the context of information security, psychological manipulation of people into performing actions or divulging confidential information.

SPAM Email that was not requested but was sent to a user and many others, sometimes with malicious intent.

SPAMBOTS Computer program designed to assist in the sending of spam. Spambots usually both create accounts and send spam messages to them.

SPOOFING When an unauthorized person makes an email message appear to be from a known sender by using either the same or a similar address.

SPYWARE Malware that passes information about a computer user's activities to an external device or person.

SURFACE WEB Any part of the World Wide Web that is readily available to the public and searchable with standard internet search engines. Also known as the *Visible or Clear Web*.

TOR (THE ONION ROUTER) Free software designed to make it possible for users to surf the internet anonymously, so their activities and location cannot be discovered by government agencies, corporations, or anyone else.

TROJAN Software that presents itself as an authentic application but carries an item of malware.

TROLL A person deliberately posting malicious or inflammatory messages with the intent to provoke a negative response.

VIRUS A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer. A file that is written with the sole intention of doing harm, or for criminal activity.

Definitions in the Glossary were principally sourced from Wikipedia. It is the largest and most popular general reference work on the internet and is ranked among the ten most popular websites. Wikipedia is owned by the nonprofit Wikimedia Foundation.

AUTHOR BIO
WILLIAM KEIPER

William Keiper is an award-winning and bestselling author of creative non-fiction. He is committed to helping individuals and businesses do things differently, as the result of seeing things differently.

He is the author of *CYBERCRISIS—It's Personal Now; Life Expectancy—It's Never Too Late to Change Your Game*; and, *The Power of Urgency—Playing to Win with Proactive Urgency*. He has published a series of short political essays: *Amazon for President*, *Apple for President*, and *Walmart for President*.

RECOGNITION

WINNER—National Indie Excellence Awards—*Best Personal Growth Book* 2014 (Life Expectancy)

WINNER—The USA Best Book Awards—*Best New Non-Fiction Book* 2012 (Life Expectancy)

WINNER—World Book Awards—*Best Self-Help & Motivational Book* 2012 (Life Expectancy)

WINNER—New York Book Festival—*Best eBook* (all categories, fiction, and non-fiction) 2012 (Life Expectancy)

WINNER—Paris Book Festival—*Best eBook* (all categories, fiction, and non-fiction) 2012 (Life Expectancy)

WINNER—World Book Awards—*Best Business Motivational Book* 2012 (Life Expectancy)

WINNER—World Book Awards—*Best Current Events—Sociopolitical Book* 2012 (Apple for President)

BOOK OF THE YEAR—Living Now Book Awards (Mind) 2012 (Apple for President)

RUNNER-UP—Paris Book Festival—*Best eBook* (all categories fiction, and non-fiction) 2014 (The Power of Urgency)

FINALIST—Next Generation Indie Book Awards—*Best Current Events/Social Change Book* 2012 (Apple for President)

FINALIST—National Indie Excellence Awards—*Best Motivational Business Book* 2014 (The Power of Urgency)

FINALIST—The USA Best Book Awards—*Best Motivational Business Book* 2013 (The Power of Urgency)

FINALIST—London Book Festival—*Best Business Book* 2013 (The Power of Urgency)

FINALIST—National Indie Excellence Awards—*Best Motivational Book* 2014 (The Power of Urgency)

FINALIST—Los Angeles Book Festival—*Best Non-Fiction Book* 2014 (The Power of Urgency)

FINALIST—San Francisco Book Festival—*Best General Non-Fiction Book* 2014 (The Power of Urgency)

FINALIST—The USA Best Book Awards—*Best Current Events Book* 2012, 2013 (Apple for President, Walmart for President)