The Art of Cyber Security

A practical guide to winning the war on cyber crime

Gary Hibberd

itgp™

The Art of Cyber Security

A practical guide to winning the war on cyber crime

The Art of Cyber Security

A practical guide to winning the war on cyber crime

GARY HIBBERD

IT Governance Publishing Ltd
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernancepublishing.co.uk

First published in the United Kingdom in 2022 by IT Governance Publishing.

ISBN 978-1-78778-366-9

ABOUT THE AUTHOR

As many books do, I should start by telling you about my business background to build some credibility. I should tell you about my 40 years in cyber security and how I have worked for many multinational organisations like GE Money, and others.

If you're interested in that, please check out my LinkedIn page:

www.linkedin.com/in/garyhibberd/.

But I'd rather start this book in a slightly different way.

Let me take you back to where my love of all things tech-related began.

At the age of nine, I saw the movie *Star Wars: A New Hope*, which dramatically impacted my young life. I quickly became obsessed with the film, and amassed all the information and toys I could relating to the franchise. But the obsession didn't end with collecting the latest duvet cover emblazoned with Luke Skywalker and Darth Vader. I also wanted to understand the mythology of the Jedi and the Sith. In my quest for knowledge, I discovered that George Lucas, the creator of *Star Wars*, took a lot of inspiration from the samurai and the samurai's approach to life and death. From that moment, I was hooked and wanted to learn all I could about Japanese culture and the samurai. Ultimately, this led me to learn about the ninja, and the martial art Bujinkan Taijutsu, which mixes physical training with history and philosophy.

In that training, I discovered how samurai lived and how they prepared for battle. When learning about military leaders, particularly East Asian leaders, it is impossible not to come across the work of Sun Tzu. This military strategist is at the core of this book, and we will return to him shortly.

At the age of 28, I achieved the much-coveted black belt, but as anyone who trains in martial arts will tell you, this is just the start of your journey. After all, anyone can 'own' a black belt, but few 'are' a black belt.

Although I have studied martial arts for the better part of 40 years, my professional passion has always been computers and technology. Again, another movie I saw sparked a passion that has never diminished: *WarGames*. This 1983 film tells the story of a young hacker who almost starts World War III when he hacks into a military base and plays a 'war game', which turns out to be more accurate than he imagined! My interest was piqued, and I wanted to understand this new world of computers and networks that was emerging. So that's what I did. I have been fortunate to work for global banks, retail, and the public and private sectors, helping them achieve higher degrees of security and data protection. I have helped shape the industry by assisting in the development of international standards like ISO 27001 (information security management) and ISO 22301 (business continuity management), and writing books or chapters for books that are educating the next generation of cyber professionals.

Fast forward to today, and I've been a cyber security consultant and data protection specialist for more than 35 years, helping companies and individuals put security controls in place that protect them and their businesses. Every day, our world changes, and security has moved from

being very operational to ever more strategic and tactical. I have increasingly seen the connection between cyber security and martial arts, and my approach to the protection of companies, data and individuals has been shaped by the martial arts I have studied.

So that's me: a martial artist who is passionate about cyber security and data protection. Now you know me a little better, let's get on with this!

ACKNOWLEDGEMENTS

I am constantly inspired by the myriad of cyber security professionals I have come across in my professional life, and I would therefore like to acknowledge their contribution here. I have learned a great deal from many of them, and I count myself fortunate to have such inspirational cyber security professionals in my circle of friends. The insights and experiences I recount in this book are drawn from my time spent with them, so I would like to thank them and to dedicate this book to them.

This book would also not have happened without the love and support of my family. My wife Sue has believed in me and given gentle encouragement throughout the writing process. Her patience and understanding of all that I do has been instrumental in helping me achieve career highs and survive career lows. I am thankful to my incredible children Luke and Jessica, who keep me honest and hold me to account for my words and deeds. I'd also like to dedicate this book to the memory of Maureen Drake, a wonderful woman who demonstrated what love and commitment are on a daily basis.

I would like to make a special mention of my friend and colleague Lee Scorey, who was there for me when it mattered most. I will be forever grateful for his friendship, professionalism and pragmatism and for encouraging me when times were hardest.

I would like to thank Yinka Akingbehin, Chris Evans, Marc van Delft and Christopher Wright for their helpful comments during the production of this book. I would also like to thank

Nicola Day, publications manager at IT Governance Publishing.

Finally, this book is dedicated to you, dear reader. People like you are daring to look at cyber security differently, and therefore will ultimately make a difference in the world. I hope you will use the ideas and principles in this book to expand your thinking on the topics of cyber security, information security and data protection. I wish you well in this endeavour, and I hope you keep this book to hand as a source of inspiration when needed most.

FOREWORD

The problem with writing is that it's so difficult to know where to start. It's hard to decide what your important first words should be. For this foreword, I'll begin by stealing (er… 'borrowing') some of Gary's words from this very book:

"Cyber criminals know where our attention is, and they are masters of deception and misdirection, attacking us when we are looking the other way. They are using every trick in the book to exploit our one-dimensional thinking. The solution? We need to improve our thinking."

AND

"Anyone can get into cyber security, just like anyone can draw. But the truly great cyber security people out there are artists. They use their hands, heads and hearts to create something special."

That's what this book is about. If you're here looking for reference architectures or step-by-step "how to be a CISO" guides, then you are in the wrong place. THIS is a book about building the mindset and approach needed to survive cyber battles, lead your army, match wits with your enemies, and successfully plan for war. The journey to acquiring that mindset begins simply enough: know thyself.

I think that's one of the main things I appreciate so much about Gary's approach to cyber security and risk management. Gary understands that cyber security is a game

of understanding strengths and weaknesses while also trying to manage unknowns. That means understanding our strengths and weaknesses, and our many enemies' potential strengths and weaknesses, and accounting (as much as we can) for unknowns. This type of awareness can be challenging to achieve – but pays off in preparedness, strength and resilience.

There are two other aspects of Gary's work that I have a sincere appreciation for. First, Gary takes a meta approach to cyber security. He begins by seeking the abstraction so as to find first principles: those fundamental truths or assumptions that cannot be deduced from any other propositions or assumptions. Then, he seeks to demonstrate how the principle applies to the specific problems we face. This is the fundamental key to helping build a mindset that will grow and flex over time, adapting (rather than snapping) as new trends and technologies emerge. I always picture this ability to adapt and flow with change as being similar to Neo at the end of the original *Matrix* movie, ducking and weaving around the onslaught of bullets hurtling his way.

The other aspect of Gary's approach that I appreciate is his continued focus on the human element. Gary knows that just because we throw the word 'cyber' about all the time doesn't mean that all of our problems and approaches to mitigating the threats involve technology. The truth is often the opposite: the mitigation critically involves understanding and accounting for humans.

And, speaking of humans, Gary is one of the good ones. I also believe that you, dear reader, are too. You decided to pick up this book at this specific time and are now reading these particular words. Something drew you to the title and topic. And now it's time to dive in. Let's get ready to know

ourselves, know our enemy and learn the art of cyber security.

Perry Carpenter

Chief evangelist and strategy officer for KnowBe4, author and podcaster

PREFACE

"To romanticize the world is to make us aware of the magic, mystery and wonder of the world; it is to educate the senses to see the ordinary as extraordinary, the familiar as strange, the mundane as sacred, the finite as infinite."

Novalis

(poet, author and philosopher of Early German Romanticism)

DO NOT SKIP THIS SECTION!

I'm going to get straight to the point: some of you will not like this book.

Not. One. Little. Bit.

Why? Because it isn't your typical cyber security book. It's going to challenge you. It's going to make you stop and think. If it doesn't, then you're going to need to reread it. This book only contains around 40,000 words and 150 pages and could easily be read in a day or two. But if you do, you've missed the point.

Take your time with the book. Once you've finished, work your way through the 'Required Reading' section at the end. Note that it is not *further* reading, because that would suggest the books are merely recommended. They are more than that. I see them as essential reading, as they build on the ideas I'm introducing here.

You may have noticed that the front cover of this book has an image of a lock with a chain and heavy padlock. But you

would be wrong if you thought I selected this image because the book is about cyber security. This book is indeed about cyber security, but it's also so much more. It's about giving you the key to your creativity. It is about releasing you from the chains that hold you down and hold you back from thinking creatively and creating something amazing. No, it's not a self-help book, but it will help you be yourself and help make the world a safer place. I'm a hopeless business romantic, which is a term coined by marketing consultant and author Tim Leberecht. Like him, I am passionate about business and believe we all have the ability to love what we do.

The aim of this book is to do just that – help you fall in love with what you do and look at our industry and yourself with new eyes.

To do this, I've broken this book into two sections; both deserve equal consideration and time. The first section discusses my thoughts about our industry and those that operate within it. I believe we are all artists, and this section explains in detail why I believe this and why I want you to believe it too.

The second section is dedicated to Sun Tzu and his influential military treatise, *The Art of War*.[1] Examining and expanding upon his words through the lens of cyber security and data protection, I would like you to consider how you can apply his thinking to your profession.

At this point, you may be wondering why there are two topics covered in one book; well, the answer is relatively simple.

[1] Throughout this book, the quotations from *The Art of War* have been sourced from the following edition: *The Art of War* (2010), Capstone Publishing, UK: Padstow.

This book started as a series of thoughts about what we do and how we do it. Over the years, I built upon these thoughts, drawing on my experiences in martial arts, at management conferences and companies I worked for, and with the cyber security sector in general. This book is the culmination of that, putting my musings in order and outlining an approach I think we should all take. I hope you can find meaning in these pages and apply it to your world, too.

Why I wrote this book: because we need it

In 2019, the UK Active Defence report stated that UK residents are more likely to be victims of cyber crime and fraud than any other crime.[2]

In 2020, BT asked more than 7,000 business leaders, employees and consumers globally about their opinions on cyber security, with some interesting results. First, it highlighted considerable confidence that suitable security measures are in place, as 76% of business leaders rated their organisation as 'excellent' or 'good' for protecting against cyber threats. However, the same report revealed that eight out of ten executives stated their employer had suffered a security incident in the past two years.[3]

For many years, it seemed as though only heavily regulated industries were interested in data protection and cyber security. From financial services to health, education and public utilities, they prioritised cyber security because their regulators compelled them. However, following a series of dramatic, headline-grabbing cyber attacks, such as

[2] *www.ncsc.gov.uk/report/acd-report-year-three*.
[3] *https://newsroom.bt.com/new-research-finds-that-the-expectations-of-chief-information-security-officers-have-never-been-greater/*.

WannaCry in 2017, many more organisations began to realise that they too could fall victim. And then 2020 happened.

The COVID-19 pandemic has further increased the risks we face, as we saw cyber criminals capitalise on the fear, uncertainty and doubt (FUD) that gripped the world. In Q2 2020, Action Fraud in the UK reported a 400% increase in reported phishing attacks, with scammers using the pandemic as a source of revenue.[4] Note that this is only *reported* phishing attacks. What about all the unreported attacks? Did you report the last phishing email that landed in your inbox? Probably not. A police officer once said to me that when a crime is reported, you should multiply the number by ten to get a more accurate picture of the crime level. Of course, this is not scientific, and we can never be sure, but we could be looking at an increase of 6,500% in phishing attacks. I'm not suggesting that we should run to the police every time we receive a phishing email, but I am saying it should be reported to someone! A phishing email is a symptom and could be an indication that something isn't quite working to filter out attempts to break into your systems. I often say to people, if you were walking down the street and someone jumped out at you every day and asked you for your wallet and your PIN code, would you report it? The answer is always yes! This is what is happening in our virtual world, yet people aren't reporting it.

So why is the reporting of cyber attacks so low? Why don't people raise the flag when they've suffered an attack? There are several reasons for this, and cyber criminals are aware of

[4] *www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march*.

them all. Let's focus on phishing emails for a second; when someone clicks a malicious link and is subject to a phishing attack, their response will depend on what happens next. They might not even notice anything has happened. For example, keylogger malware downloaded from an infected email will sit quietly in the background collecting information, and the victim will be unaware until days, weeks or months later when they are alerted to some fraud. If the payload is ransomware and the victim's device or information is made inaccessible, the first thing the user will do is call their IT support person – whether that's their child, partner, friend or IT department. Next on the list is likely to be the bank to inform them that their accounts might be compromised. If the phishing email contains malware or ransomware, the victim might even call the police. But what about corporations that fall victim? Why aren't they calling the police or Action Fraud? Yes, some will inform the police as they may have insurance policies requiring a police case number, but the response is often internally focused. Why? To put it simply: brand protection.

If a cyber attack hits an organisation, the reality is that there will be a heavy focus on brand protection and damage limitation. It may sound cynical, and there are exceptions to every rule, but when a CEO or business owner tells you *after* a breach that security and data protection are their number one priority, they are not telling you the whole truth. We've seen this countless times over the decades, where a breach has impacted organisations and customers only hear about it months later, after the company had "completed internal investigations". If security and data protection were truly the number one priority, the business would have informed customers at the earliest opportunity, when it discovered the breach, so they weren't left at risk from cyber criminals. But

they often don't, preferring instead to conduct internal investigations to find someone to blame, speak to their lawyers or insurers, create a positive marketing campaign to drown out any negative press, and perhaps sell shares in their company before the news breaks.

Cyber criminals know all of this and capitalise on it.

Why I wrote this book: because I needed to

As I said above, this book grew from thoughts I had over many years, It began when I first started studying martial arts, which was around the same time I started down this technological path, in the early 1980s. I saw a lot of parallels between the cyber security professionals, martial arts and artists that I worked with and trained with. Anyone who studies martial arts for any length of time will most certainly come across the military strategist Sun Tzu, who is credited for writing a series of documents that became *The Art of War*, or more accurately 'The Art of Strategy'. Although his words on military strategy, tactics and operations were written more than 2,000 years ago, I am often struck with how relevant his words are today.

The longer I work in the cyber security sector, the more I am convinced that every cyber criminal must at some point have read Sun Tzu and is using his teachings against us. This is an important point that I do not want you to miss. As you read the pages dedicated to Sun Tzu, I want you to place yourself in the mind of both business leaders and a cyber criminal. You'll quickly see that ignoring the words of Sun Tzu could leave you at greater risk of attack.

These thoughts have occupied my mind and shaped my career for the longest time, and the more I thought, the more I knew I needed to write them down. I started writing this

book because I wanted somewhere I could collect my ideas on a topic I have been passionate about all my life. It started out as a series of short blogs, notes, and opinions on security and privacy, but each section grew a little longer and more reflective as I wrote. Although I love what I do, there have been times when I forgot how important and impactful our roles are. I also found it challenging to find new ways to learn, inspire or think about our discipline so that we think about it differently. It's essential to do this to keep our interest and passions in the job high, because if we're not, how can we expect anyone else to be?

So the notes I wrote became pages, and those pages became this book. In writing it, I want to reignite a flame in you for these topics, which may have dimmed over the years or even gone out altogether. It happens to the best of us, me included.

I wrote this book to challenge your thinking on key topics and force you to approach cyber security and data protection from theoretical, philosophical, strategic, tactical and operational perspectives. But I also wrote this book as a 'love letter' to the industry and to all those who serve within it. Although there are countless books about cyber security and data protection, there are very few (if any) about you and me, the professionals. I believe those who are successful in this field are tenacious, passionate, knowledgeable, dedicated, caring and hard-working but frequently undervalued, unappreciated and misunderstood. The first part of this book is dedicated to each of us who have felt this way. It is a reminder of how astounding our profession is, how significant our roles are, and our individual contribution's brilliance. I want to inspire and encourage you when you feel like all is lost or when you're feeling undervalued and unappreciated. It's a section that I wish someone had given to me when I felt this way.