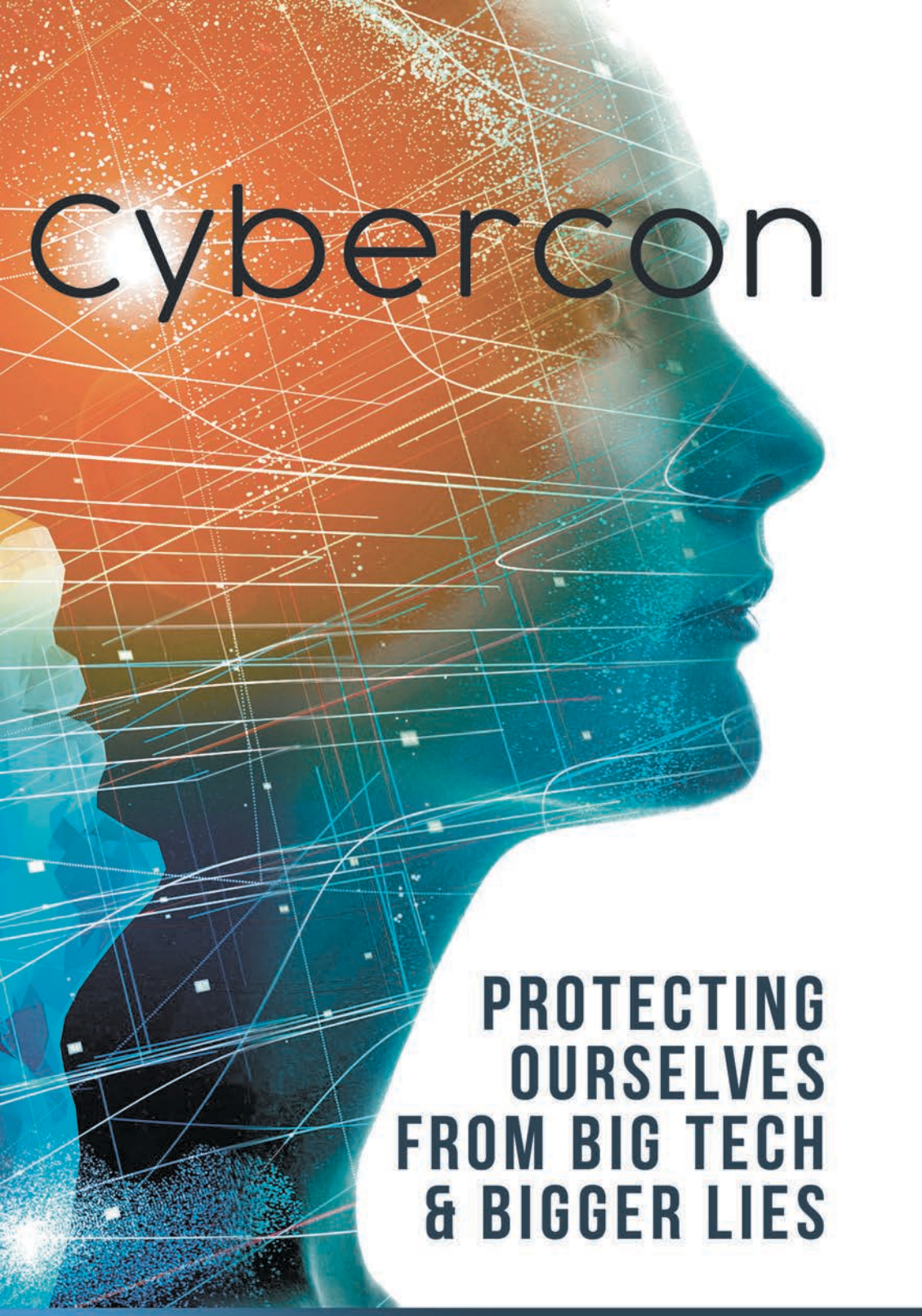


Cybercon

PROTECTING OURSELVES FROM BIG TECH & BIGGER LIES

DR. JAMES L. NORRIE

Cybercon

Cybercon: Protecting Ourselves from Big Tech & Bigger Lies

Published by Mindstir Media, LLC

45 Lafayette Rd | Suite 181| North Hampton, NH 03862 | USA

1.800.767.0531 | www.mindstirmedia.com

Printed in the United States of America

ISBN-13: 978-1-7342210-9-1

Library of Congress Control Number: 2019918962

Cybercon

PROTECTING OURSELVES FROM BIG TECH & BIGGER LIES

JAMES L. NORRIE

ENDORSEMENTS

"Excellence in People, Process and Technology have always been the keys to a successful organization. However, when it comes to cyber-threat management, the emphasis by most has been on process and technology, not people…with increasingly disastrous results. In his latest book, Dr. Norrie identifies underlying reasons for the "people risk gap", providing a structure and framework to enable a more effective cybersecurity strategy for the human risks present in all organizations."

—Craigg Ballance
Retired Bank Executive & Director,
Canadian Member Services FS-ISAC

"Do parasailing and cybersecurity intersect? Learn how when you read this book! Fascinating. A heartfelt ground-breaker that convincingly transforms cybersecurity conversations from fear to hope…"

—Carol-Ann Hamilton
Best-selling author, consultant, speaker,
and national radio show host

"In business today, we have done everything we can to secure technology and still there are breaches. The missing component is the human element of cybersecurity which this author explores in a compelling and convincing way that will help us all stay safer online. Well done!"

—Mark Ripplinger, President & CEO, Everlink Payment Services

"Cybersecurity keeps executives up at night, wondering if they will be the next headline-making victim of an unfortunate cyberattack that hurts their customers and harms their brand. Given we are all just one click away from scandal, I recommend this book to any leader of any organization…it provides a blueprint for mitigating the human side of cybersecurity, something most organizations are simply missing."

—Barry Clavir, Founder and CEO, Leader's Beyond Inc.

"Buy it. Read it. Do it. Genius!"

—Tracy Abbott, Chief Compliance Officer

"As someone who does not truly understand the intricacies of the world of technology, I found this book very revealing. It gives voice to many of my own fears, and offers hope for the future. It is inspired reading for anyone concerned about society's collective online destiny."

—Dr. Judith A. Kirkpatrick, retired Professor, Dean and Provost

"Once again, Dr Norrie cuts straight to the root cause of contemporary online hacks with a refreshing change from the usual fear-mongering to an innovative approach that encourages education and cooperation."

—Stuart Grant, Chief Compliance Officer

"If you want to fight hackers, change tactics. Cyberattacks are more prevalent than ever, touching work and families all the time. Big Tech & Bigger Lies can help you SAVE yourself from yourself and protect your money in an age of increasing cyber vulnerability. Upgrade your online behavior today!"

—Kyle Reid and Cheryl Purves, Small Business Owners

"As a cybersecurity professional who consults about keeping organizations safe, I am always striving to learn about the latest advances in our field. Time and again we blame cyber breaches on the technology, which fails to recognize the human element that is ultimately the most important factor. This book solves that puzzle!"

—Ajay Randhawa, Cybersecurity Consultant

"Are you at risk? Or maybe your family or workplace? This book addresses our human vulnerabilities online, and Dr. Norrie offers innovative strategies to combat these issues helping make surfing safer for us all."

—Harley Ranson, Retired Aviation Engineering Executive

DEDICATION

To all the cybersecurity professionals and academic colleagues I know who really get it, working to keep us all safer online. To my patron, Chloe Eichelberger, whose generosity, inspired intellect, and spirited debate nurtured my early thoughts on this subject. To my patient and loving partner who is my biggest fan! To my family, and especially my Mom and daughters—sometimes far away but never far from my heart - and dear friends, who when I promised to never write another book, supported me in this adventure anyway. I love you all for so many wonderful reasons, but all the more for this kind indulgence!

TABLE OF CONTENTS

PROLOGUE 1

INTRODUCTION: The Wrong Approach to the Problem 5

CHAPTER ONE: Cyber as a State of Mind 13

CHAPTER TWO: The Test 23

CHAPTER THREE: The Results 33

CHAPTER FOUR: Tone from the Top 51

CHAPTER FIVE: Why Can't I Just Buy CyberInsurance? 63

CHAPTER SIX: Under Attack from Within 75

CHAPTER SEVEN: Getting Naked Online 91

CHAPTER EIGHT: Improving Cybersecurity Awareness 99

CHAPTER NINE: Big Tech Ethics – Finagling, Favors, and Fines 109

CHAPTER TEN: The Geopolitics of Cybersecurity 123

CONCLUSION: 137

PROLOGUE

We all have an online history, and mine is directly related to this book. As the owner of a business that depends on the internet, I can recount first-hand just how important cybersecurity is. But there is more to my story that is directly relevant, so let me begin by going back to the fall of 2016. I received a call from our IT manager. The panic in his voice was palpable…

Customer traffic to our website had been geometrically increasing for almost two years because of our razer-sharp focus on rolling out a robust global digital footprint. This took considerable energy and resources. But with online success came the unavoidable security issues we always anticipated, and thought we had thoroughly prepared for. But that phone call turned that naive assumption on its head as we experienced our *first* fully blown digital nightmare.

Our website had been successfully hacked. It came crashing down right in the middle of the critical holiday shopping season – something my business really depended on. No new leads, lost holiday sales, and no interface for our customers. In pre-internet terms, our beautifully designed store on 5th avenue, enticing huge numbers of passersby's to come in and browse, became instantly invisible and the front doors locked. No storefront. No window display. No signage. Everything was

gone. It was scary.

After the mad scramble to recover, I obsessed with a multitude of questions. Why us? Who would do this? We're not a big bank or a public company. Was this some random Australian high school student with too much time on his or her hands since that is where the attack had started? Or was our traffic being hijacked to a "money site"? Maybe this was the devious work of a jealous and malicious competitor? Or an attempt to mine our large database of sensitive customer information?

In the end, it turned out to be the latter - this time by Russian and Ukrainian automated bots mining our site for rich data which, fortunately for us, wasn't linked in any way to our website. We were lucky.

My after-the-fact response to this incident is what any business owner would do. I demanded the implementation of a host of expensive Fortune 50 level security protections. Although I knew this wouldn't make us bulletproof (no one really is), at least we would become *significantly* less vulnerable, maybe able to sleep a bit more soundly at night knowing we had done everything we could.

Or at least I thought so. Until that fateful fall day of 2019. I had just gotten back from the gym and pulled out my cell phone to check my email. A new message had just been sent from one of my most trusted senior staff. It read:

> Subject - Wire Transfer Confirmation
> Hi Alan,
>
> Here is the wire transfer confirmation.
> They should have the funds tomorrow.

I was horrified and called immediately asking - WHAT TRANSFER??? The confident, almost indignant "what do you mean what transfer!' voice explained details of the $43,000USD transfer to another country that had been processed per my instructions in a series of emails exchanged between us throughout the day. Of course, predict-

ably, the problem was I had not sent any of those e-mails.

Then came silence. My employee had been carefully and artfully spear-fished using a spoofed e-mail address that was hauntingly close to my real e-mail ID. It was an easy mistake, a human error. But this loyal employee now realized she had been duped.

There followed a horrified "OH MY GOD ALAN" followed by a gasp filled with excruciating terror and embarrassment. What to do next?

Again, luck was on our side. The transfer had only just been authorized with our FX partner, and not yet forwarded into the foreign bank account. So we were able to quickly recall it. But a mere matter of minutes later and the ending to this story would have been entirely different. And the outcome would have generated a substantial and unrecoverable business loss for which there was no recourse.

This was my second cyber unawareness epiphany. It unfolded just exactly as described inside this very book. Today it's not enough, not ever going to be enough, to protect your IT assets with the very latest and most sophisticated cybersecurity technology. That alone cannot keep us safe, although that effort has value. Instead, I learned my own lesson the hard way. The next wave of digital warfare will certainly be waged with computers and technology, but not targeting us directly from outside the organization, but rather indirectly using our most precious assets - human beings – against us from the inside.

Dr. Norrie has understood this, and has been teaching this new reality of human hacks to business leaders for many years, passionately beating the warning drum that no amount of time or money spent on technology tools, punitive threats, or even generic awareness training about these new threats will ultimately *change behavior*. Our biggest cyber threats will now come in the form of sophisticated and pernicious attacks that target basic human vulnerabilities. And he has produced a powerful and *holistic* system that comprehends that reality with practical solutions that actually work, aligned to each of our individual personality traits and online instincts. He takes this fight personally and it shows.

On hearing my tale of cyber woe, my friend shared his manuscript, test and training plans with me in its early days. In fact, he eventually shared them with my whole company. And it worked. I was the very first organization to pilot his then evolving system, and it could not have been more timely or valuable. I read his book in wonder at the timing of his writing effort and my recent breach: with each new page, it gave voice to my worst fears, but also provided hope and positive solutions that we might all eventually prevail and make ourselves safer online. I felt better just for having read it.

I have now seen these transformative tools at work. When my employees understand what types of online threats they are most vulnerable to, and are given the tools to check and double check methods to mitigate those threats, we are all more secure as a result. We have created a culture of "we're all in this together". And what company couldn't use an increased dose of that?

While mine is only one story, and personal to the author and me, I also think its representative of what is really happening in the world. ANY business – or individual or family for that matter – is at risk of being exploited online. That threat is growing and so is our fear.

As the author so eloquently notes, our growing use of technology only makes us more vulnerable. Throwing more technology at this problem will not solve it. Yet, we also cannot also live in a state of constant fear or complacency either. Instead, only each of us can solve this dilemma by empowering ourselves with new knowledge and new approaches. This book does that. I urge you to read it and internalize its message. Then take the test and start to figure out how you can keep yourself, your family and your organization safer online, because that benefits everyone, everywhere.

—Alan Merriam, CEO
Merriam Music
Toronto, Ontario

INTRODUCTION:
THE WRONG APPROACH TO THE PROBLEM

Cybersecurity is **not** primarily a technology issue. It is a human behavior problem on a massively networked scale. Denial of this fact, driven by the drumbeat of Big Tech profits and false promises, is not productive, does not keep us safe online, and works to society's detriment. This book explores how and why this is happening and what you can do about it. It is about empowerment rather than victimhood, sweeping away online fear and replacing it with hope.

When humans perceive danger, a natural physiological *fight-or-flight* response is triggered. Fears about online cybersecurity risks provoke this autonomic stress response, and it is not under our control. Rather, this instinct developed as an evolutionary response over centuries for the self-preservation of our species. That means every single one of us is somehow affected whenever we enter this state, whether or not we recognize and accept it.

Hyperarousal, once triggered, instantly washes our bodies in bio-chemicals that heighten our senses. These bio-chemicals include cortisol to enhance blood sugar, increase our blood pressure, and sup-

press the immune system to temporarily increase energy. Testosterone to boost strength; dopamine and serotonin to enhance brain function and suppress our normal pain response; and adrenaline to support the immediate physical response of either fight or flight. These hormones are powerful chemicals: if they were pharmaceuticals, they would surely be controlled substances requiring a prescription!

Of fundamental importance to this book is the notion that hyperarousal, and its associated condition of hypervigilance (an enhanced state of sensory sensitivity accompanied by an exaggerated intensity of behaviors whose purpose is to detect dangerous activity), trigger a state of increased anxiety-causing *complacency and exhaustion*. As we become complacent and exhausted, we make increasingly worse decisions about dangerous situations. This can result in an endless loop of stress and anxiety, including and perhaps especially when we are online.

By nature, this mental state must be *temporary* because our bodies cannot sustain this condition for prolonged periods because of its negative biological consequences. Research has shown that if this state is perpetually triggered, eventually we become less and less able to withstand it, becoming *desperate* to return our bodies to a normal state by eliminating, escaping, or ignoring our fear. In extreme cases, it can cause a yearning for death, a highly dangerous state of mind with its own set of attendant consequences leading to higher rates of mental illness and suicide. Sound familiar? Two decades of statistics now prove an increasing trend for both of these outcomes around the world, without a satisfactory explanation yet.

But I suspect a strong connection to our growing online social behavior because we are truly engaged in a grand human experiment. Yet, in this current period of technology development, the long-term consequences of this experiment remain a mystery as we proactively disintermediate human physical and social connection and replace it with technology substitutes. This cannot help but subtly affect human evolution over time. As a species, we are always adapting our underlying human condition to match our environment to improve survival. This will be no different of course.

As with any longitudinal social change, the human impact and societal consequences of this shift will take decades to emerge. But they will. And while social science research methodology makes it hard to claim a measurable cause and effect relationship among these changes, it seems intuitively obvious that as technology-induced fear increases, so does widespread generalized social anxiety. How that impacts society will depend on how we all adapt our social responses over time.

As part of the human condition, we do not relish being afraid. We rather seek to avoid it. But today, this fear is autonomously triggered by simply living in a tech-laden social environment that virtually demands participation. Whether we like it or not, simply by being aware, we gain knowledge of new technologies and their inherent risks. We then delve into this technically enabled artificial world embedding these lurking fears ever deeper into our psyche.

This makes it possible for the plague of cybercrime, political manipulation, information overload, and online anxiety that pervades the internet today to trigger hypervigilance in most of us. Big Tech contributes to this fearful state of mind by offering an array of ever-expanding social media platforms and similar technologies, unregulated and unrestricted, to create a globally interconnected, but also potentially more dangerous, world.

In response, many cybersecurity professionals in the workplace, who I know care deeply about protecting the information assets of their organizations, give in to this fear, perhaps embracing and supporting it as a way to enhance individual awareness of cybersecurity risks. This translates to an outcome—*whether we are at home or at work*—where we feel perpetually, perhaps subconsciously, afraid of technology. And this is dangerous because it exhausts us.

More of us than ever live in some state of this sustained fear, whether or not we participate in online activities and platforms. As peer pressure to be present online grows, users begin to depend on these systems for a variety of new online social activities and outlets, perhaps even believing they *need* them to be socially connected. Researchers refer to this as technology-intermediated social transactions—and they

function differently than those we seek and maintain in person. This means just going online triggers broad personal, professional and social impacts.

As we examine this topic together, I will explore how this impacts our mental health, emotional stability, and psychological conditioning. I can prove technology changes our behavior at work, and that has implications for an organization's cybersecurity efforts. Later, I will also link this state of fear to increasing rates of depression, suicide, domestic terrorism, religious radicalization, and global political interference on a grand scale. I will present how it haunts our elderly who are especially vulnerable because of technical naiveté, leading to cruel hacks and attacks which leave them feeling more alone, socially embarrassed, and broke. And we will explore the ever-present online dangers for our youth, who may not have sufficient developmental experience to properly understand and manage their online behavior.

Regardless of the cause, this constant state of fear underpins many important social consequences that are interconnected in cause and effect creating impact on every single one of us, both personally and professionally. Technology progress is now erasing hope in vast tracks of society as we simply become resigned to being afraid, manipulated and deceived online.

So while selling the value of their new digital inventions to investors and consumers, Big Tech denies responsibility for these consequences. And they actively deflect efforts by government regulators to bring them to account too. They depend on our unbridled sharing of personal information of all sorts, both appropriate and inappropriate, and actively attack anyone who criticizes them—including me—as Luddites who must not understand the democracy-building characteristics of new social technologies that rise above tyranny and censorship to invite self-expression. But that argument is ultimately self-serving. And false.

Of course, there are kernels of truth in the defense that not all technology is bad. It can deliver on some of its promise and potential. But Big Tech generally overpromises and under-delivers, and therein

lies an important truth: the introduction of all this technology is what creates cybersecurity risk in the first place. Cybersecurity exists as a massive and costly worldwide problem simply because online technology exists on a similarly massive scale.

So how do these self-proclaimed "technology breakthroughs" really benefit society versus enriching the companies that produce and promote these leaky platforms? We know from public disclosures that these companies are benefitting economically at unprecedented rates from our "free" use of their platforms. But what proof do they proffer of positive impacts to offset the abundant proof of the negative impacts these technologies are imposing on civil societies around the globe? This gap represents a real human cost of incalculable proportions.

Why? Because complete online cybersecurity is *never* possible. It is a myth. All systems are vulnerable—it is only a question of degree. So long as systems are ultimately designed, operated, and inhabited online by humans who are frail and vulnerable, there will be mistakes. Therefore, simply being online brings some level of inherent risk to each of us because we make mistakes. All we can do is mitigate these growing risks through sensible participation and awareness. And most of us already do that in our offline lives anyway: we balance overall risk and reward and are self-managed when and how we choose to engage in risky behavior.

Technology companies, and any company that operates online actually, possess personal information about us that others would like to steal and exploit. To keep us confident in sharing this information with them, they make us believe the answer to increasing overall cybersecurity lies in enhancing technology to make computer networks safer. But they know there is no guarantee, so they hint at their innate ability to keep us safe online, trying to overcome our fear of participation. But what they are really doing is protecting their ability to grow their own profits. That goal will always come first, driving another important conclusion of this book—commercial self-interest drives corporate behavior and decision-making.

Some consumers may prefer to deny this obvious conclusion. They

continue to participate in Big Tech's artificially crafted online worlds, enjoying what benefits that may bring, but always assuming they should be able to hold someone else accountable for keeping them safe online. If they ask us to share personal information, surely these companies know how to keep it safe, right? But that is a misplaced vote of confidence in Big Tech. More sophisticated companies may know more about how to keep your personal information safe, how to ensure that systematic backups prevent risk, and how to build redundant systems to increase service levels. But not all companies either know how to or can apparently afford to do so. That is why these attacks succeed, and why they are never going away because there will always be frailties and vulnerabilities as technology and humans intersect and interact.

The truth of the matter is, technologists have done everything they likely can to this point in purely technical terms, yet it has not kept online participants safe. So we are all just only one click away from disaster most of the time. I conclude that the biggest risk involving technology is not the technology itself, but human use and abuse of it. Therefore the dominant cybersecurity issue is not *technical* hacks but *human* hacks.

Technology-based cybersecurity efforts today, no matter how intense or sophisticated, cannot protect us from *self-inflicted harm*. Systems engage innate human behavior—both good and bad—and unlike technology, the human condition is complex, immutable over centuries of evolution, and is not easily predicted, interdicted, or controlled.

This obvious frailty—because humans are flawed—is the truth that makes our fear about these platforms so valid. Social media especially are susceptible to exploitation simply because they assemble humans, who are unpredictable and can be dangerous, into a technically intermediated and largely unregulated online ecosystem. Mistakes will happen, and harm will occur by definition. As we experience or hear about more and more unfortunate incidents online, the associated negative impact of learning about this makes us more and more afraid. This naturally triggers our fight-or-flight response. And the cycle begins and repeats.

Yet the state of hyperarousal/hypervigilance that online technologies trigger in humans is ultimately counterproductive. To overcome it, we must become empowered to understand and manage the risks these social media platforms *individually* represent, and those are *quite personal to each of us.* To accomplish that, we must learn more about ourselves, becoming self-aware of the risks we inherently undertake when we go online, learning to mitigate and manage them for our own benefit. We can't rely on a company, more interested in profits than people, to do this for us. And that is the *"cybercon"* referred to in the title of this book that Big Tech wants us all to buy into. But it won't succeed because society is beginning to figure out these essential Big Tech lies and broken promises, rapidly calling them out for what they are.

It is self-deceiving to think anybody but you can save you from your online instincts. While government regulation, potential new laws, and questioning Big Tech motives are important issues to explore in this book, the personal value of *cyber self-regulation* cannot be reinforced enough for the benefits they bring to you, your family, and to organizations.

So this book can help everyone become more cyberaware. It pro-

poses self-directed safer online practices aligned to your instincts and habits. It demands you get engaged in global cybersecurity issues that are rapidly arising in novel ways. These can have potential personal impacts you must be aware of, not afraid of. And I conclude that mastery of *technology-induced fear* is ultimately the surest path to curbing recurring, risky online behaviors successfully. Acquiring new knowledge and perspectives can help each of us overcome fear by taking appropriate actions to reduce personal risk. We become part of the solution, not the problem.

Ultimately, this is the most significant Big Tech lie: while they can help us *stay safer online* technically, they cannot make us personally *behave more safely online*. Cybersecurity is ultimately a personal pursuit, and Big Tech knows it. It is up to each of us alone to achieve.

In mastering these nuances of behaving safely online, I intend this book to help you feel less afraid, more in control, and ultimately more effective at cybersecurity than you ever thought humanly possible. I want internet participation to be safe, fun, and productive for all. I want to protect and preserve technology innovations for the greater social good instead of greater evil. To accomplish this requires we all transform user fear into hope, making cybersecurity a very personal social and human mission globally.

CHAPTER ONE:
CYBER AS A STATE OF MIND

Technological progress is inevitable, and as Moore's Law defines, relentlessly exponential. Especially in the recent course of human history, society has experienced the rapid ascent of technology. But is that pace of technology change now outstripping society's ability to adapt? Human evolution takes time, and we are on the cusp of a startling Fourth Industrial Revolution that will not treat all of society equally well[1]. As a result, technology progress will turn into social disruption, and trigger unforeseen and unintended consequences. In fact, some inventors report deep regret as the true risks of the technology they created later emerge, and as widespread adoption imposes unintended consequences on all humanity. But ignorance of this only breeds fear. Instead, we need to explore it and use new knowledge to inspire hope.

We sit at a critical inflection point in terms of current cycles of tech innovation and disruption as it relates to social media platforms. Facebook—the mother of all social media platforms literally—was only

1 See the informative video from the World Economic Forum: *What is the Fourth Industrial Revolution?*

founded in February 2004. That makes it less than twenty years old as a technology; but, frankly, it seems like it's been around forever, doesn't it? And that is part of what technology progress does. It culturally envelops us, and before we know it, we embrace it without due regard to the potential good and bad that adoptive impulse creates. This is particularly true when the technology has no cost and spreads virtually and virally as Facebook and others have done globally. Before we know it, they **are** the de facto status quo and they exert powerful social, political and economic influence as a result.

However, we should be mindful that online social behaviors are simply adaptations of how humans have always behaved. They are not really new. For instance, where we had crimes like theft, fraud, and impersonation before Facebook, we have them on Facebook today. And we will have them after Facebook when that time comes when Facebook too fades into human history. That is because these systems simply *transfer* existing human behaviors into *new online forms*. For example, social engineering is simply basic fraud—one of the oldest tricks in the human history book—but masking in new online disguises. This demonstrates social media technology as enabling human potential for both good and bad, mirroring our innate human nature. This also suggests not becoming over-wrought with fear about all this – its just a normal part of human nature that has been with us for centuries actually.

Of course, Big Tech only promotes the positive potential of their latest inventions, often denying obvious negative social impacts, even when they are obviously visible. That is what good marketing does: it accentuates the positive promise of any new product. Further, everyone really wants to secretly believe the marketing hype and assume new technology must be good technology. To do otherwise risks being labeled anti-technology—someone who simply "doesn't get it." But perhaps you *do* get it, harboring a deep-down niggling sense this isn't just quite right and that it could lead to bad outcomes. You are slowly entering a state of hypervigilance.

Over time, constant media coverage of the cybersecurity risks of

new technology confirm your looming fear that there are online dangers. Stories spread and evidence mounts of these platforms enabling cyber bullying, real-time online group suicides, boastful sharing of criminal activity as a badge of honor, and recruiting of domestic terrorists to inflict mass shootings on innocents. Reports show the multitude of illicit ways criminals prey on our innocent children, teenagers, and our elderly particularly, exploiting their sense of trust in these social platforms for criminal gain, inflicting great personal harm to many.

In this environment, our initial giddy sense of progress is replaced with dread: what has been created and why did they do that? A sense of retrospective loss replaces the anticipation of the joy of progress as new tools are used in new ways to perpetuate old deeds, continually proving the darker side of humanity. But the human condition itself has not changed—only the speed and scope of the online platforms available to demonstrate its evil side has.

Contemporary culture and mass media often treat all of this as new. It is not. These human behaviors have always been present and were always a risk. Moving online, they just present more often because of the ease of reaching billions of people worldwide in a single click from any place in the world now. And that scale is the only really new part to this story.

The thing that has really changed is speed and how easy these negative exploits are to accomplish, reducing the friction required for humans to engage in hurtful, demeaning, or criminal acts globally by targeting millions of us all at once. This is the "progress" we have been pursuing in creating a completely technology-enabled and interconnected planet.

Of course, claims of the good these platforms engender are fair. Some aspects of new technology can expand human horizons and create positive changes. But as with most things throughout history, the speed of evil adoption seems always to outpace the good, and negative news is more swiftly shared than good news. This contributes to our gnawing fear. So, we tilt away from anticipation of the good to an overwhelming sense of dread about the bad. But if we only worry

about risks, we never end up having any fun—and that's sad.

So, we have to understand this instinct as opposed to simply giving into it. We know it can provoke a continuous sense of hypervigilance, risking escalation to hyperarousal, inviting the natural fight-or-flight response that is so much a part of our human condition. Remaining locked in cycles of detecting and responding to fear and danger is not sustainable; so, we seek ways to resolve this state even if they are not always helpful. The options can include withdrawal from participation in what we perceive as a dangerous activity; attempting to mitigate or reduce the fear of harm or perceived dangers; imposing controls of constraints to make ourselves feel better when we do undertake the activity; or simply ignoring the harm and potential danger and engaging in the behavior anyway, accepting whatever consequences that brings.

I want to pause for a moment. It is this last option—avoidance—that creates the most dangerous online cybersecurity outcome for most people and what I worry most about from my research. *It means we participate fully while suppressing signs of danger ahead.*

In presentations, I refer to this as a **cyber state of mind**: *blissful participation tinged with willful ignorance*. This is an obviously dangerous state of mind that increases our online risk and leads us astray. But being in a more aware state constantly triggers uncomfortable biological reactions we yearn to avoid. So, through denial, we enter this cyber state of mind to reduce our inherent sense of looming danger. Yet, as this cycle becomes self-perpetuating over time, managing these feelings is at the very core of enhancing our personal cybersecurity.

In a repressed state of denial, we engage with technology feeling almost normal, deliberately dinting any looming sense of danger. We continue online behaviors without grasping fully the real risks they represent, moving into an almost trance-like state of using something for whatever purposes we feel are urgent and important enough to tempt us into participation while ignoring danger. We have been lulled into complacency.

This means we lose sight of how to keep ourselves safe, especially where simple modifications to our online behaviors might mitigate

risk and legitimately make us feel less afraid. Ironically, being afraid now drives us to *cyber ignorance* making us more vulnerable to the very things of which we are now afraid. That is substantively ironic to me.

What should we do? To properly secure the relief from hypervigilance we biologically crave, we must become more self-aware of our particular technology-induced behaviors and when they promote or demote our online safety. We must learn how our personal online behavior makes us more or less vulnerable and why each of us potentially exhibits a unique set of online risks. For ease of reference, I adopt the term "cyberaware" throughout—a state of being more reflective about how more informed use of new technologies can help us feel less afraid. Essentially this means acquiring new knowledge about our existing online instincts.

By accomplishing this, we begin to disassemble and then reconstruct our own online behavior. We are enabled to compare the risks and rewards of how we are behaving instead of blindly adopting new technology just because. We can *choose* how we are going to adopt, or not, various technology innovations for our own future benefit instead of Big Tech's.

By rejecting wholesale adoption of new technologies across society until we resolve cognitive concerns about their implications in advance, we all become more personally empowered to modify our online behavior in response to technology changes over time. *This maximizes our personal gain while minimizing our risk*. Notably, this is also exactly how humans approach this problem in the offline world.

Witness, for example, being on vacation and seeing others parasailing over the warm waters of the Caribbean. They appear to be having lots of fun. You do not see any obvious evidence of danger after watching them from your perch under a beach umbrella. Because you have never done this before, you are naturally *cautious*, but not necessarily afraid. At this point you arrive at an inflection point: you might, for instance, decide to look online for statistics about how safe parasailing is. You discover negative coverage indicating just how dangerous this activity is. As you research further, you discover stories and videos

showing actual injuries or fatalities from this activity. Your mind begins to race. Remember, you haven't decided yet IF you are going to do this particular activity; rather, you are investigating the risks and rewards of that potential decision. Depending on your risk tolerance, you may dismiss parasailing as an option, and returned to the safer realm of reading a book on the beach. Or, if you are more risk-tolerant or torn, you may still be in a state of cautious consideration.

Continuing, you venture closer to a final decision and walk toward the kiosk where the activity is booked and paid for. You speak to the attendants and learn more about both the rewards (fun, fun, fun!) and the risks. They explain what they do to ensure your safety, perhaps handing you a list of safety and security features they claim (training, life jacket, experienced personnel, specially designed non-tangling harness, etc.). Of course, they leave until the end the legal waiver you will eventually have to sign ensuring that you are responsible for the decision you are about to make, accepting no liability for any personal injury or death!

This description, even if you have never parasailed on a beach, should be reminiscent of how you actually approach a decision to engage in any new activity. You compare the risks and rewards and self-determine your level of comfort. If the activity seems too dangerous, your flight response will kick in, and you will abandon any idea of participating, perhaps literally running in the opposite direction! Or, if the activity seems to offer more potential for benefit and fun under the sun, and you perceive the risk as manageable, you shake off the fear and sign up.

Whatever your decision, it is an inherently *personal one* over which you have complete control. It should not be about following the crowd because that requires giving into peer pressure, also not good, and more likely as a provoking factor in our behavior as kids or teenagers. Instead, as adults, we must adjudicate this decision on its own merits, and on a risk-adjusted basis. We each use our own intuition after securing facts about how this decision may impact us either way.

Seemingly we abandon these important checks and balances when

it comes to our instincts about new technology, apps, or social media platforms. As others adopt it in a frenzy of enthusiasm—online invitations to participate overflowing your inbox and peer pressure to post increasing—you feel left out unless you immediately accept and engage. You repost, share, and invite others wantonly pushing ever more of your personal life online. That is peer pressure.

Left aside is taking time to determine for yourself how you may or may not benefit from that online participation, and social judgment being what it is, you may sense negative social consequences will arise, secretly fearing rejection if you elect to sit it out. So, you dive right in and initially, our participation seems innocent, fun, and maybe even interesting. However, in the back of your uncontrollable mind is a sense of dread about what you are doing. Might it be dangerous and pose unknown risks? You may even learn something you innocently did online is now reported as being a risky behavior, making the fear conscious[2]. All this cumulatively intrudes into our psyche triggering that ever-recurring fight-or-flight response.

What now? Well, you continue to participate because you have already decided to do so—but your brain is crying out for you to reassess and rethink your decision. Maybe it's not safe! So, the biological trap becomes obvious: this is not a sustainable state for very long because we do not like feeling afraid, and something has to give to reduce these feelings of anxiety.

As I stressed earlier, a first step is to properly evaluate risks and to take the time to do so *before* participating. That definitely helps. However, often with new inventions or applications, we have neither the time to do so or access to the information about the real risks and results of participating, before we feel drawn into this peer-driven web of participation.

2 See for example: https://www.vox.com/the-goods/2019/7/17/20698271/faceapp-privacy-panic-russia-old-face-filter-app

One thing most of us have is a natural instinct toward assessment of risk and reward that underpins how we react in various situations. We are all either risk seeking, risk neutral or risk averse to some degree. Come to discover, this is an inherent part of our trait-based personality. So, your own inclinations on this are easily detected and examined if you take the time to do so, particularly made easier if you are prompted for what to look for.

For anyone who has been through psychotherapy, this process of uncovering, examining and then repurposing our innate, instinctive responses is a first step in changing them for the better. Or trying to anyway. But most of us need a stimulus to provoke this journey of self-discovery before it can occur. Maybe this book can serve that purpose for your online behavior.

Given our inherent personal calculus as it regards risk and reward, once we understand this, we can potentially adjust our online behavior accordingly to stay within either self-defined safety limits or limits your workplace might establish, for instance. This helps you feel less vulnerable leading to less perceived danger, thereby reducing fear

and enhancing your online experiences. Similarly, as we collectively all achieve this state, we begin to experience more positive rather than negative outcomes from our technology participation, enhancing our sense of calmer acceptance of our own technology decisions.

What can be concluded from all this? Big Tech should *not* be allowed to dictate our social participation in their inventions. That should be a personal decision for each of us, exercised thoughtfully and with a complete understanding of the inherent risks and rewards. Peer pressure arising from the rate of adoption of any particular new technology should not be a factor in your personal adoption decision, because not all new technology is good technology. Or, a technology that is good for one person may not be good for another. We must learn to choose.

Reserving these as strictly personal decisions prevents drift into complacency. Otherwise, a self-depleting *negative cyber state of mind* is triggered by forced acceptance of technological progress, participating whether we like it or not. The goal of this book and the test it describes is to help you gain knowledge that empowers you to be safer online, triggering hope and displacing fear so you make better technology decisions in keeping with your instincts. In so doing, we all become less of a risk to ourselves and to others, making online activities safer.

CHAPTER TWO:
THE TEST

For as long as humans have existed, they have exhibited their own individual personalities. As diverse as the DNA that creates our physical characteristics, the make-up of our personalities is a blend of nature and nurture in a constellation of traits in combination that create the dimensions that make each of us unique. Personality defines our personhood.

Of the many ways of examining all that, the psychology I prefer is trait-based personality theory. Most psychologists and sociologists agree that trait-based theories have face validity. This approach can help us better understand ourselves. When properly applied, this theory can describe and explain personality similarities and differences in understandable ways, although there are limitations to this approach just because of the sheer diversity of minute differences in personality humans present.

Nonetheless, it is superior to most other theories such as Freud's psychoanalytic or humanistic approaches and, generally, more accessible to people because they recognize the language in trait-based theory

as easily self-applied. And who hasn't taken a personality test at some point in their lives and been amazed at the results? Moreover, if you picked up this book, your natural interest in this subject may have had you do many of these for many different reasons over time just because there are so many behavioral assessment tests.

Thus, it became intriguing to me as a researcher to think about how trait-based personality theory might explain our online behaviors—our cybersecurity profile, as it were. Was it possible that how we behave online and the risks that we run are more aligned to underlying personality traits rather than simply being random? To what extent is our behavior a question of nature—less changeable—versus nurture and experience—and therefore more changeable?

This journey of discovery led to study just about every trait-based personality theory and the many associated behavioral assessments derived from them starting around 1952 until about 1980. At this point, the field became both saturated to some extent; but also quite stable as a well-accepted and validated theory within psychology. Simultaneously, as a society we became quite intrigued by testing, particularly standardized testing, as a way to sort ourselves out.

This research path led me to discover and establish a new approach to detecting, predicting, and interdicting dangerous online behavior, both individually and collectively through standardized testing. At the outset, personality theory was too diverse and had too many traits to easily correlate them to our online behavior—it needed to be simpler to be effective as a predictive tool. This led to an exploration of which specific personality traits most likely affect your actual online behavior. Two very relevant personality traits emerged that consistently show up in how we behave online: the degree to which we are either *risk-tolerant or risk-averse* and an attendant desire and willingness to generally be either a *rule breaker or rule follower*. I wondered: could these two dimensions be reliably assessed and discriminated individually?

If these two specific traits could be detected and predicted successfully, it would help particularly explain why some individuals are more or less prone to third-party inspired exploitations where they

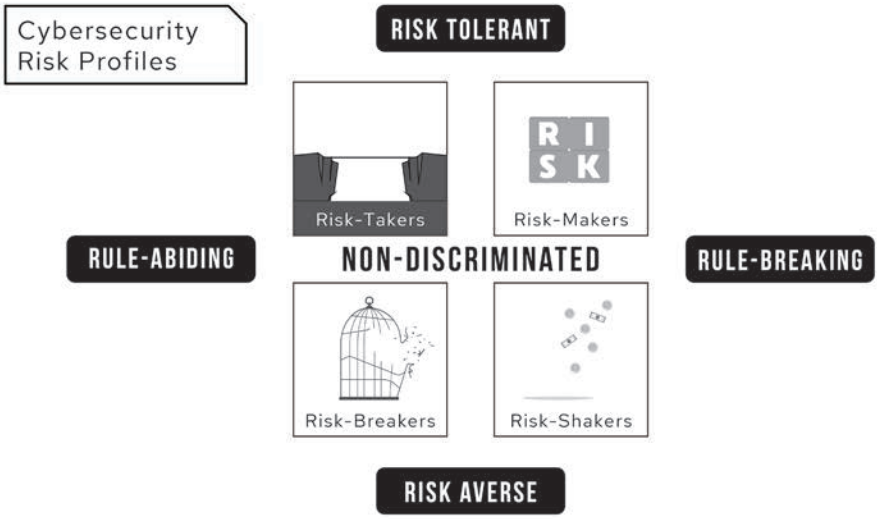
respond to or click on something online when they should not, or are somehow induced to share something online when they should know better. Wow!

These two particular axes began to form the basis of my evolving theory on how to profile the cybersecurity risk of any individual, specifically in an on-the-job context. This is increasingly urgent and important in a globally interconnected business world full of online cyber risks, and where so many people and companies daily report being hacked or attacked.

Using a subset of educational testing theory, I was able to eventually isolate and evolve a series of non-invasive test questions that, when ranked by respondents on a Likert scale between 1 and 6, were seemingly predictive of their underlying inherent approach to risk-taking and rule-following behaviors. Through pilot testing, eventually responses to their items were reliably linked to specific traits and were translated to what is essentially a snapshot of an individual's online risk. This breakthrough has since been patented, now proving to be reliable about 93.7% of the time as individuals report a high degree of self-agreement with the test results.

As with any instrument, in about 4.3% of cases, the standardized test can only successfully detect the dominance of one of the two traits and is less equivocal on the other, forcing the respondent to self-identify the more applicable profile. And, the test fails to discriminate less than 2% of the time because the individual exhibits a central mean tendency that makes their presentation of differences so slight the test cannot detect them successfully. That does not mean they do not exist, only that they are intensely moderated. The automated testing method can even detect a respondent who is deliberately trying to provide a pattern of responses instead of being truthful through item intra-correlation. So the test works!

The results of my **CyberIQtest** then deliver a personal cybersecurity profile that locates you in one of four quadrants that I chose to label for easy reference to each specific style:



From the illustration you can see that an individual's profile is derived from the extent to which they are either risk tolerant or risk averse on the one hand and rule-abiding or rule-breaking on the other. The test measures your instincts on these dimensions to locate your base personality in one of the four quadrants, or as non-discriminated if you are too in-between.

Further, within each of these quadrants, the test can further detect the strength of expression of the traits associated with that quadrant, resulting in either a moderate or stronger expression within the quadrant—that is, pushing outwards toward the furthest boundary of the behaviors. The labels I chose are tied to the nature of each quadrant to provide a conceptual framework for understanding our innate cybersecurity risks. But I must be entirely clear on an essential point: while each represents a relatively higher or lower risk of being prone to certain types of online exploitation, *anyone* in *any* of these quadrants can be hacked.

The more relevant question is to what degree is someone in a par-

ticular quadrant likely to fall prey to what specific types of online hacks and attacks? Also, no one style is *better* or eve *superior* at avoiding attacks, just less vulnerable to some particular kinds of attacks. Or more likely to be more easily trained to avoid their most likely vulnerabilities for example. And they disperse across the quadrants in different ratios in different industries and businesses I have found. So this means there is no "better" test result to have, one over another.

That is because *all* organizations need employees that exhibit *all* four traits because these inherent personality traits apply to many other dimensions of on-the-job behavior besides simply adhering to risk-reducing practices. Therefore, the test is **not** about eliminating a specific kind of person from the organization in order to reduce or control the risk of a cybersecurity incident. Rather, the test can identify specific types of cybersecurity attacks (known as threat vectors) that are *more likely to succeed and why* given any particular individual's particular risk/rule profile. These also creates the opportunity to consider overall rates of risk prevalence and preponderance to risk for the entire organization by mapping its organizational make-up according to the range of people found in each quadrant:

This can provide those tasked with managing risk and compliance in an organization (or your extended family, church, or club too for that matter) the opportunity to refine optimal mitigation and interdiction strategies across the whole organization by implementing "style-aligned" training and controls for example. So this book and the test are a compliment and adjunct to other cybersecurity efforts already being undertaken. Why is this important?

Because it adds a novel dimension of *personalizing* risk mitigation and control that reflect your individual personality. This new knowledge includes the ability to self-assess one's own most risky online behaviors in a new way. It helps *sensitize* you, and any organization to which you belong, to the likely kinds of third-party cybersecurity hacks and attacks you more easily fall prey to—and to which you must pay particular attention when engaging online.

This knowledge empowers everyone within an organization to self-detect and reflect when they are approaching a risky apex or decision point. Instead of hypervigilance—which as we learned is unsustainable and not always helpful—we can apply *focused awareness*, a condition which *is* sustainable and of real risk-mitigating value. Taking this test helps us detect and avoid situations that are potentially harmful so we worry less about those things that are less likely to be a threat. This brings welcome relief from the constancy of fear that occurs if we believe that all online activity and every act we undertake online is likely to harm or hurt us. The test contours our ability to be empowered against online risks becoming more cyberaware.

The transformative impact of knowledge arising from the test also gives an individual language to compare and share their online behavioral profile with others—family, friends, or colleagues, for instance. As we venture to discuss the *relative risks* of our particular personality and our resulting online behavior, we come to realize that the risks and rewards of being online are variable and uniquely apply to each of us personally. The reduction or elimination of generalized fear and anxiety is a very productive outcome of this approach, enabling a more empowered feeling that contributes, properly, to a now growing sense

of online well-being.

While it is clear that no test can entirely eliminate online risk for an individual, it is *entirely predictive* of the kinds of behaviors and attack vectors that are likely to succeed and ensnare you. That is powerful knowledge. And as imperfect as this method is at preventing all harm, isn't it leaps and bounds better than constantly worrying about everything you hear about as a risk online? By enabling online risk assessment in a more self-aware way, you focus on the more relevant threats to you personally and emerge feeling more empowered to be in control.

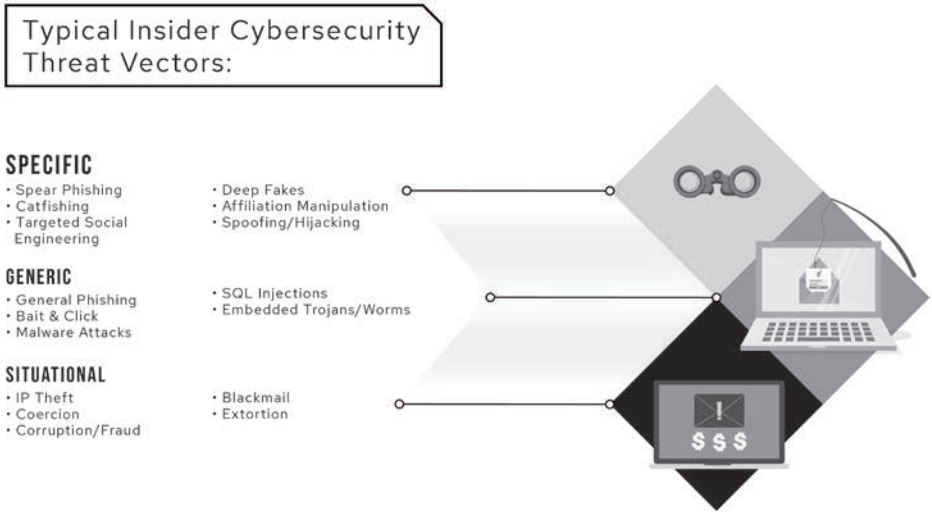
Worth noting is that this test will **not** detect what someone who has access to your online information might fail to do in securing and protecting access to it. That is simple negligence. And it cannot detect those with criminal intent who are hiding in order to perpetuate fraud or theft—because that is deliberate deviance. This test cannot unmask false intention.

And technology is still imperfect with flaws and failures that can be exploited to hack into systems and steal your information if you have provided it to an organization for any reason. That is never going to change. However, excellent efforts by so many talented cybersecurity professionals are slowly eliminating brute force technology attacks and exploits as the primary source of most cybersecurity breaches today anyway, leaving human hacks as the real threat.

So, this test is aimed at reducing human error—and because we are imperfect—this is the source of more and more of the reported cybersecurity attacks now successfully taking place, and particularly those that involve real economic harm.

Obviously, human-inspired attacks are hard to prevent because they arise from human behavior which is not easily predicted or controlled. Among cybersecurity professionals, it is known these human-factors can never be completely eliminated as a risk. Therefore, any claim by anyone to 100% completely secure systems is impossible to achieve. It is also clear these threats will change and evolve over time, since once we discover one variation and try to eliminate it, creative folks

on the other side will come up with a new variant. However, common third-party inspired attacks do fall across a range of established threat vectors today that is useful to understand, each one associated with labels and their own description as follows:



Most attacks of this sort involve convincing an employee or other insider of an organization, or a family member for that matter, to do something they shouldn't such as providing access to systems through either turning over their credentials, compromising security or password protections, clicking on an attachment that downloads a virus or malware, or being subjected to a deep fake, shaming, or outright extortion for example. In all these instances, *the common weakness that is exploited is human not technical.* You can find lots of additional and up-to-date information on the most current types of online attacks online and from many sources. Of course, just make sure you are getting your information from a reliable source and not being duped by conspiracy theories, false information or being baited by hackers trying to lure you in!

Human factor attacks are often the most damaging kinds of cyber-attacks—because someone always has the "keys to the kingdom" as we

say in the tech biz. And if a lock has a key, it can always be opened. If a person can be turned, perhaps even while remaining completely loyal to the organization or with no intent of being exploited, then cyber predators bypass all of the fancy technology protections and often achieve unbridled access to personal information and company secrets. This is what really creates the opportunity for most cybercrimes to occur.

As more organizations recognize this, they learn they cannot continue to rely solely on technology measures to maintain cybersecurity. They then become more interested in this test and other means to help them work with their employees to detect when they are being improperly influenced online. By doing so proactively, they are less likely to trigger a dangerous cybersecurity breach. This is the logical next step in cybersecurity compliance and control even as uncomfortable as this conclusion might be for its human implications. Why?

Because adding a human dimension to compliance and risk management efforts may seem somehow unfair to those being profiled for risk, and this is understandable. But it is not intended to be punitive but constructive and empowering profiling. And any negative feelings cannot stop us from proceeding with this approach either, because not doing something we could do also leaves us feeling uncomfortable, right? We must accept that we are all susceptible to different kinds of risks and online exploitations just because our personalities are all different. The more we know about ourselves, the safer we can make ourselves online.

Further, many of us already take various kinds of other tests to classify us and clarify various things about our aptitudes, skills, and abilities in other areas of our lives. Think about IQ tests, for example. Why not relate it to cybersecurity and our online behaviors?

Ultimately to be more effective, we must stop assuming that profiling without a malicious intent is bad by definition. We must separate inappropriate or misguided profiling—such as racial profiling for example—which we should not do because of its negative societal consequences. It is also inherently unfair and biased. But this test is *not* that kind of profiling.

Instead, it is a helpful tool for both the individual and their organization to deploy so long as it is constructively used to promote safer online practices through awareness and training and not for discriminatory purposes such as hiring and selection. That is because, as you will see for yourself, every single style has value and worth within the organization and is necessary for it to perform properly. Diversity of online style is no different than the many other forms of diversity we promote in organizations that have inherent value. We need to simply accept the risks of everyone's style and improve collective cybersecurity—not for them to leave the organization!

Obviously, I cannot guarantee how people will end up using this test because it is published and available commercially so they can use it however they want to. However, it is my hope that those who take it will enjoy it, learn from it, and benefit from its potential positive impact. But with any new technology, I acknowledge there is always a risk of inappropriate use.

Now that we have discussed the underlying theory of the test itself, let's move on to explore how it can be applied.

By the way, if you are interested in taking the test for yourself please visit **www.cyberconthebook.com** for more information. I am convinced you will be amazed at what you will learn.

MORE INFORMATION

To understand more about the test and its practical applications for you and your family, please visit

CYBERCONTHEBOOK.COM

For organization-wide programs or cybersecurity consulting based on our patent-pending methods, visit our corporate site at **cyberconIQ.com.** Here you will find cost-effective ways to implement the test and accompanying online training to immediately improve your company's overall cybersecurity risk profile and compliance.

If you would like to explore having Dr. Norrie do a keynote at your event or company, please visit **cyberconthebook.com/bookings/.**

For up-to-date information about cyberconIQ and the latest cyber security trends, please follow us on social media:

@cybercon.thebook

cybercon.thebook
or
cyberconiq

BIG TECH IS RESPONSIBLE FOR A BIG LIE: WE ARE NOT SAFE ONLINE.

Their innovations are self-proclaimed as progressive, convenient, and community-building. And sometimes they are. But in reality, we are more like lab rats in a grand human experiment with unpredictable and potentially harmful consequences. While Big Tech prefers to deny and deflect, these huge global technology platforms provoke fear, cause social disruption, and enable information manipulation paving the way for hacks and attacks that wreak havoc in our lives.

Reporting on ground-breaking research, Dr. Norrie explores how personality traits such as your innate sense of rules, risks and rewards dictate online behavior. These make us all more or less vulnerable to cyber predators suggesting today's really important cybersecurity questions are less about technology and more about simply being human. Inspiring hope, the author offers easy to understand strategies and tools that empower us against these threats, making us all more cyberaware. Align your technology choices to your personality keeping you, your family, and your organization all safer online; because Big Tech can't or won't do that for you.

DR. JAMES NORRIE is the founder of CyberconIQ Inc. former Dean of Business and now professor at York College of Pennsylvania. This is his sixth book. His proprietary CyberIQ test predicts your personal cybersecurity risk. A noted expert, he makes frequent media appearances, speaks, writes, and consults globally about how tone from the top, improving cyber situational awareness, and other high-impact practices reduce organizational risk by making cybersecurity a team sport. His mission is to tilt the global conversation about social technologies toward hope and dissipate fear by modifying our online behavior, mitigating third-party human hacks, and making the internet a safer place for us all.

MINDSTIR MEDIA
www.mindstirmedia.com

U.S. $16.99
ISBN 978-1-7342210-9-1
51699
9 781734 221091