Foreword

In my 20+ years of adventures working, learning, and contributing to both the information security and intelligence communities, I can still say I have only met a handful of noteworthy leaders. I guess that's to be expected since they say that true leadership is quite rare… but should it be? In the information security field, it seems more than rare. Security leaders seem almost non-existent. Is that because there aren't people capable to lead in this space? I don't think so. We see highlights of leadership all around the Information Security community. We see open-source initiatives such as Offensive Security's freely available Kali Linux Distribution, which provides an all-in-one pathway for learning and performing penetration testing and digital forensics. We see SANS taking the lead on the quest to offer scalable advanced Information Security education. We can't forget all the open-source tools, that have been pioneered, that inspire more than half the commercial technologies of today such as Metasploit, Bastille Linux, Tripwire, BeeF Framework, Bro, Security Onion, Snort, Suricata, Mozilla Defense Platform, OpenBSD, SELinux, and to name just a few.

And then you have our individual security leaders that literally believe in protecting our security (and sometimes privacy) communities and by boldly doing so create disruptive advances within our industry. The first one that comes to mind is security leader

Katie Moussouris, who used her skills to courageously stand up for hackers and security researchers and their misunderstood community by literally pioneering an entire industry for them. This allowed their abilities to be demonstrated and valued as a positive benefit instead of something to be feared. While she was at Microsoft, she creatively designed a solution to the very complex and long-standing problem of vulnerability research and disclosure management. Katie put in place bug bounty programs that incentivized hackers and big corporations to do the unthinkable and miraculously work together willingly. This solved not only the logistical problem of scaling vulnerability disclosure and management through hacking policy, but it tapped into the heart and soul of a human issue: the legitimate elimination of rejection the majority of hackers and security researchers encountered due to non-acceptance, fear, or misunderstandings. Through cooperative game theory strategy and a deep sense of empathy and ingenuity, Katie instead bridged that gap, and also created a freelance marketplace for hackers to thrive personally and professionally based on their skillset. A game-changing win–win. Katie continues to lead as the authority in vulnerability disclosure and bug bounties as an expert for the U.S. National Body of the International Standards Organization (ISO), and she led the charge in helping the U.S. Department of Defense start the government's first bug bounty program.

There are a few others that have fought the good fight and created industry, or law, or policy. People like Phil Zimmermann and Jon Callas of PGP (Pretty Good Privacy) fame; we have folks like Richard Clarke and Howard Schmidt that championed cyber national security policies for the White House. Yet, the real rarity is the day-to-day leadership. The success of consistency without glory and fame. The required discipline to maintain the passion over the onslaught of politics. The reality that the leader serves the team, and not the other way around.

Now bring in the security aspect and then we have to not ignore the elephant in the room: ***the Information Security ego***. We cannot deny it. Worse, it is encouraged in our community. The security leader, the CISO in most cases, is expected to know everything.

And that is why I am very excited that this boldly written yet extremely (maybe even aggravatingly) informative and much-needed work is finally here!

But first, a ***word of warning***: before reading this book, you will need to leave that Information Security ego at the "LOGIN" prompt. Otherwise, you will not even come close to receiving the real game-changing insights this book can provide. I therefore implore you to go in as if you were a beginner in your field. Tap into the young ambitiously curious good old days where you didn't see hard or easy, but only an opportunity. Go in with no preconceptions, and definitely don't take the book personally unless it's where you see you can personally apply and improve. Then get ready to gain a new perspective that may shift your thinking with great benefit to you, your organization and the constituencies that you serve.

On a personal note, I've had the honor of working with Barak Engel throughout my career. He has brought me a lot of opportunities I can truly say I wouldn't have otherwise had, and more importantly those opportunities together provoked and invoked constantly new perspectives for me. These perspectives that Barak would impart literally impacted my career in such that it pivoted me from someone who excelled just as a technologist and advanced technical security geek to a balanced information security professional. He got me to think beyond the bits and bytes, which not only enhanced my logical-to-lateral thinking abilities greatly, but I also learned business strategy, social intelligence, perception management, and even political de-escalation techniques that to this day help me achieve the best success of managing risk by encouraging transparency and discouraging passive aggressive political plays within the organization. To put it bluntly, the successes I have had within the organizations I've worked with (e.g., Head of Cyber at Deloitte, as well as taking multiple companies to acquisition, running my own companies, and currently as Chief Scientist and acting lead handling risk management/Information Security for Flashpoint) regularly include the philosophies asserted in the book you are about to read.

This book isn't about technology. It's about getting away from it. It's about not treating a symptom, but instead solving a problem beyond the vacuum of what we think is Information Security. Why is it that 20 years later we are still trying to solve the same problems that we didn't solve back then? And then, only to find everything more challenging and disappointedly reactionary. If you're bored at your job because of this, then you should be. Why, because that's boring.

It's not creative. It has no strategy. It has no element of ingenuity. It's throwing the next promised technology at a problem in a tactically reactionary manner with no benefit and only added stress and frustration on you and your team, and actually… wait for it… added risk to the company.

If you're ready to get out of that repeated rut, then this book nails it. If I had an analogy, CISO expectations today remind me of the business of medical doctors handing out the newest pharmaceutical medications to their patience until something sticks. This brute force mentality is not very hacker-like. It's definitely not creative. It incorporates precisely zero strategy. And likely in the long run will produce limited success.

If this book had a subtitle, it should be: The De Facto Common Sense Strategy Guide for Organizational Risk Management. The way Barak brings this perspective surprisingly simplifies the over-thinking, over-working, and over-political life of a CISO by demonstrating how the security leader truly gets to be the leader, the advisor, the sage, and the arbitrator for the entire business itself. This shift of the role finally empowers the CISO to break beyond the political barriers, and ***lead with fury*** one's vision of security and risk management to its success, from planning all the way to execution. It pulls the EQ out of the IQ and overlays them neatly so that one can see the pragmatic decisions that need to be considered, but while encouraging and enhancing the creative side of solving these problems more with people instead of just technologies.

For the financially savvy types, the insight in this book can literally lower your TCO when it comes to security management and monitoring costs by looking the what the real bottom line actually is… in other words, your people at their finest.

Who knew?

For the policy and compliance oriented, you are definitely covered. From effective approaches for scaling data classification to map to your current Information Security policies, all the way to business continuity development and ensured execution.

What I love the most about this book is the fact that it isn't a book about being just a CISO, and how to be one and why they fail. It's a book about leadership through genuinely learning to understand your people successfully. I'll admit, my team and the people on it come

first and foremost. I've taken massive political hits to go to bat for my team, and I will continue to do so if required. This book's most vital takeaway is in the fact that it doesn't ignore the use of social intelligence or the actual psychology perspective of managing risk. Essentially, this book was written with heart and wasn't really written for the CISO's gain, but mainly for the teams you continue to serve.

It has been an honor to be asked to write the foreword to this book. Because this book is humbling… and caring… yet confident, creative, and courageous, the exact qualities required for leaders to evolve to what we truly could be.

I will leave you with one of my favorite quotes from Thomas Jefferson:

> One person with courage is a majority.

Thank you Barak Engel for this book. Enjoy the read!

With honor
Lance James
Chief Scientist
Flashpoint