CYBER RISK IS BUSINESS RISK

MARQUE

PUBLISHING

At Marque Publishing, we believe ideas deserve to become reality.

Every project we publish is built on one simple idea:

Our mission is to help bring dreams to life.

We are living it every day, and we invite you to join us on the journey.

www.marquepublishing.com

CYBER RISK IS BUSINESS RISK

You can delegate the decision, but not the liability.

Chris Thatcher

Foreword by Sam Rehman

Marque Publishing

Published by Marque Publishing, LLC
Wellington, Florida

ISBN 979-8-951546-03-6 (hardcover)
ISBN 979-8-951546-04-3 (paperback)
ISBN 979-8-951546-05-0 (ebook)

LCCN: [pending]

Printed in the United States of America

First Edition

The information in this book is provided for educational and informational purposes only. It does not constitute legal, financial, or professional cybersecurity advice. Readers should consult qualified professionals for advice specific to their circumstances. The author has made every effort to ensure the accuracy of the information at the time of publication, but laws, regulations, and technology change rapidly. The author assumes no responsibility for errors, omissions, or changes that occur after publication.

Some names and identifying details of individuals and organizations in the case studies have been changed or omitted to protect confidentiality. Where cases are drawn from public record, court filings, or published government advisories, they are cited as such.

To my wife, Dannielle – Thank you for being my partner in life and raising four amazing children with me. I never could have had this career without you taking care of what matters most at home.

To my daughters, Jordan, Lexie and Nicole. I am so proud of the strong women you have become.

To my son Jayden. You are the reason I get out of bed every morning. I love you.

Contents

†

Foreword

†

We all like answers.

In fact, we often want them too soon, immediately, and in too much detail. It's human nature. When uncertainty arises, especially regarding safety, our instinct is to resolve it immediately. To move. To react. To do *something*. And sometimes that's absolutely the right thing to do, assuming you have the right training and experience.

But over more than thirty-five years in this business, leading organizations through incidents and helping clients navigate some of the most difficult moments of their careers, I've learned something that seems almost counterintuitive.

The best leaders don't begin with answers. They begin with a pause, however brief, and then questions. They observe. They listen. They separate signal from noise and ask the questions everyone else overlooked.

I've made it a personal objective to study how people react during a crisis. A cyber incident has a way of compressing time. The room fills with emotion, stress, urgency, and instinct. It amplifies everything. Everyone wants to act. Everyone wants certainty. Everyone has an opinion. Yet in those moments, the

most valuable person in the room is often the one who speaks the least.

In many ways, this book is about learning to separate signal from noise, clarity from confusion, and thoughtful leadership from instinctive reaction.

†

Years ago, while I was serving as a CISO, I was hosting a roundtable dinner for security executives. Before the evening began, I noticed one of the attendees—a CISO I'd known for years—sitting quietly by himself in the corner. That wasn't like him.

I walked over and asked if everything was alright.

He looked up and said, "Actually, no."

Then he asked me a question I've never forgotten.

"Sam, I've spent years building this security program. My GRC team tells me our framework maturity is excellent. Our assessments consistently rank us among the strongest organizations in our industry. Every dashboard tells me we're doing well."

He paused.

"But three days ago, LockBit brought our entire company to its knees. Our operations stopped. Our people couldn't work. I don't even know if I'll still have a job next week."

Then he asked quietly, "How can both of those things be true? How can one part of my organization tell me everything is going well while another reveals we're completely vulnerable?"

That question has stayed with me ever since.

The answer isn't that frameworks are wrong. They aren't. Governance, risk management, and compliance are essential disciplines. Strategy matters. Architecture matters. Boards and the executive team need that view. But that's only one side of the coin.

The other side lives on the ground—in the security engineers and analysts responding to alerts at two in the morning, collecting evidence, orienting the group, calming everyone down, patching systems, containing the attack. I could go on and on. The operational realities never quite fit inside a dashboard.

Great security leadership lives in the connection between those two worlds, a balancing act that never takes its eyes from either side of that coin. Strategy without operational truth creates false confidence. Operations without strategy creates chaos. And the connection between them can't be built once and forgotten. It has to be continuously maintained, challenged, and recalibrated as the organization changes and as the threat landscape evolves.

Reading Chris's book, I found myself thinking back to that conversation. Much of what he writes is really about closing that gap—helping executives understand what the dashboards don't say, asking better questions, and making sure the view from the boardroom reflects what's actually happening on the ground.

That's leadership. That, to me, is what I've always called The Anchor in the group.

†

That is why this book is worth your time.

There are countless books that explain cybersecurity. Far fewer explain leadership under uncertainty. Chris has written the latter.

What makes this book different is not the technology. Technology will change. AI will evolve. Attackers will find new methods, and regulations will continue to mature. Those details matter, but they are not the lasting lesson.

The lasting lesson is that cyber risk has become inseparable from business leadership. Today's executives are expected to make decisions about resilience, operational continuity, AI governance, and risk tolerance—without needing to become cybersecurity experts. Chris understands that reality. Rather than overwhelm you with technical depth, he gives you a framework for thinking, for asking better questions, and for leading with greater confidence.

I especially appreciate that this book doesn't rely on fear. It relies on perspective.

The stories are real. The lessons are earned. The questions linger long after you've finished each chapter. More than once, I found myself reflecting not on what Chris was telling the reader to do, but on how many of these conversations I've witnessed myself over the years. Different companies. Different industries. The same leadership challenges.

AI has only made that harder. We're heading into an era where decisions have to be made faster, with more uncertainty

and greater accountability than ever before. In that environment, leadership will be defined less by having immediate answers and more by the discipline to pause, understand, and ask the questions that matter most.

As you read these pages, don't focus on finding all the answers immediately. Pay attention to the questions. The right questions expose assumptions, create clarity, build trust, and lead to better decisions. And when the next crisis comes—and someday it will—it may not be the person with the loudest voice or the quickest answer who leads your organization through it.

It will be the Anchor.

Sam Rehman, CEO Hitachi Cyber

Author's Note

†

Between the time I finished writing this book and the time it reached your hands, the next thing arrived. It always does.

In April 2026, Anthropic announced that it had built an AI model capable of autonomously discovering and exploiting software vulnerabilities that had gone undetected for nearly two decades. The model was so capable that Anthropic made the extraordinary decision not to release it to the public. Instead, they gave it to a small group of cybersecurity partners and told them to find as many holes as they could before someone else did. Within weeks, that group had identified more than ten thousand critical vulnerabilities in production software running the world's infrastructure.

By June, the U.S. government had imposed export controls on the technology. Cybersecurity professionals published an open letter arguing that the restrictions were taking the best defensive tools away from the people who needed them most. Competitors scrambled to build their own versions. The policy debate was still unresolved when this book went to press.

I'm not telling you this because this particular model is the story. By the time you read this, there will be a newer model, a

bigger number, a sharper debate. That's the point. The cycle I described in these pages (enthusiasm, adoption, lag, incident, regulation, hard-won discipline, and then the next wave) is already turning again. Faster than the last time.

Appendix E is my field report from inside that turn: what frontier models changed about the work, and the three major investments serious enterprises are funding in response.

The questions haven't changed. The urgency has.

— Chris Thatcher

Wellington, Florida

June 2026

INTRODUCTION

"Son, I Have No Idea What Any of That Means"

†

The bank president stood up slowly from his chair at the far end of the conference table. He was in his seventies, old school, the kind of man who built a regional bank in North Carolina on handshakes and relationships and the quiet confidence that comes from knowing his business down to the marrow. He had people he trusted to handle the things he didn't understand, and he'd never pretended otherwise.

My team and I had just delivered our final presentation, the capstone of a year-long security engagement. We'd done good work and I was proud of my team. We'd taken his bank from a place of real vulnerability to a defensible posture, and our slides showed it: security metrics, technical findings, remediation timelines, risk assessments. The works.

When I asked if there were any questions, the room went quiet. Then the president looked at me and said:

"Son, that was an impressive presentation. But I have no idea what any of it means to me and my business."

I was taken aback. We'd spent a year on this. But the moment he said it, I knew he was right, and more than that, I knew the problem wasn't his. It was mine.

He smiled and asked me three questions of his own.

"How much did I spend?"

Roughly $650,000.

"I am a simple country boy. I don't want any of your fancy technical jargon. Give me a letter grade the way they do in school. Where was I when we started?"

I told him the truth: borderline failing. A D-minus.

"Where am I now?"

A solid B.

He nodded. Then he asked the question that changed how I think about every conversation I've had with a senior executive since:

"Do I need to be an A?"

I thought about it. And I told him the truth again: *"No sir. Spending more on the residual risk will give you a diminishing return on investment. Mitigating the risk of unlikely events which would have minimal business impact doesn't make business sense."*

He said thank you, and he walked out of the room.

That was more than twenty-five years ago, and I've never forgotten it. Not because the bank president taught me something about cybersecurity, he didn't know a firewall from a fence post. He taught me something about communication. About the gap between what security professionals know and

what the people who approve budgets, and ultimately bear responsibility for security decisions actually need to hear.

I started as an IT director at a Big Five accounting firm and eventually moved into consulting. Doing the IT audit work is what grounded me in the consulting mindset that has been with me through my entire career. This is also where I developed the questions I asked in every CFO interview at the end of my security controls audit. The roles I have held since, leading security practices, selling security technology, helping large enterprise clients solve complex business problems securely, have allowed me to see things from distinct vantage points. Through all of it, one consistent observation: the executives who make the business decisions about cybersecurity are almost never getting the information they need in a language they can use.

The bank president figured that out in thirty seconds. He didn't need to understand the technical details. He needed to understand what he'd bought, where he stood, and whether he needed to do more.

That's my promise to you with this book.

If you're a CEO, CFO, board member, or any executive responsible for your organization's security and compliance, this book is for you. My intention is not to make you a cybersecurity expert. I will arm you with the right questions and help you frame the answers so you can make informed decisions about the risks your organization faces.

More than twenty-five years later, the questions the bank president asked are still the right questions. Every executive who

carries responsibility for an organization's security posture has to answer some version of them. *How much did I spend? Where was I when we started? Where am I now? Do I need to do more?* The questions are durable. The conditions under which executives now have to answer them are not.

Things are changing faster than at any point in my career. When the bank president asked his questions, the window between a software vulnerability becoming known and an attacker exploiting it was measured in years. Today the typical case is five days. The meantime to remediate known vulnerabilities is still five months. That is the math that has changed. The math problem is confirmation, cybersecurity is not a technology problem, it is a business problem.

The decisions the security team is making about fixing problems carry real business risk, so you need to understand the risk and make the decision about what is acceptable. For a long time the consequences of delegating those decisions were manageable. That is no longer true.

Regulators and courts have caught up. The SEC now requires public companies to disclose material cyber incidents within four business days. Courts have expanded the fiduciary duty of oversight to include cybersecurity as a mission-critical risk. CISOs have been criminally prosecuted. CEOs have been personally sanctioned. The consequences of getting cybersecurity wrong have become personal for the executives in charge, and AI is a big part of what is driving that shift.

The bank president understood his job. He listened to the answers and made the decision. He did not ask his security advisor whether the bank should be an A. He decided. The job hasn't changed. The world you'll be deciding in has.

The World Has Changed

I've been saying that cybersecurity is a business risk, not a technical problem, for thirty years. For most of those years, I felt like I was shouting into the wind. Executives nodded politely and went back to treating security as an IT problem. When success is a non-event, it becomes something to be funded reluctantly, and given serious consideration only after something went wrong.

That is no longer possible.

AI has changed everything. Not in some abstract, futuristic sense. Right now, in your organization and in the bad actor community.

AI is fundamentally transforming how enterprises operate. Every major software vendor has embedded AI into their tools. People across your organization are using AI to boost productivity, many of them without approval, without controls, uploading sensitive data into public models and making business decisions based on outputs that have not been validated. This is shadow AI, and most enterprises have no idea how much of it is running.

Outside your walls, the same technology is being used against you. AI does at machine speed what used to take attackers months: automated reconnaissance, AI-generated phishing and

deepfake attacks that are virtually indistinguishable from the real thing, adaptive and autonomous attacks built to evade your detection technology.

And this is the part that connects everything else in this book. AI is not just changing the threat landscape. It is the catalyst that forced regulators to hastily draft new regulations in an effort to catch up. The speed and scale of AI-driven risk is why the SEC wrote four-day disclosure rules. It is why courts are expanding fiduciary duties to include cybersecurity oversight. It is why enforcement actions are naming individuals, not just institutions. It is why insurers are rewriting their policies with AI-specific exclusions and why seventy-two percent of CISOs now refuse to take a position without personal liability coverage.

And the place where all of it lands is on the desk of the executive who carries responsibility for the organization. That is what this book is about.

What You Can Expect From This Book

You don't need to become a cybersecurity expert, you need to demand information from your security team in terms that allow you to treat cyber risk the way you treat financial, market, and operational risk. That means treating security as a business continuity and organizational resilience question, where the decisions about risk tolerance and operating speed stay in the executive room rather than getting delegated to the security function.

Every chapter is anchored in a real story from my own career or from well-documented public cases. I don't believe in theory without context. These stories include a CFO whose first instinct was to cover it up (it got worse) and a CISO gone rogue by vibe coding his own solutions, and we will go through some real cases where executives faced personal or criminal liability for failures that took place on their watch.

Throughout the book we will come back to a set of questions that I started asking early in my consulting career. I started asking the questions to create tension without fearmongering. They are questions that force you to confront what you don't know, and the potential business impact if your assumptions turned out to be wrong.

The bank president in North Carolina didn't need a cybersecurity degree. He needed someone to translate. He needed letter grades, not acronyms. He needed to know where he stood, what it cost to get there, and whether he needed to do more.