THE CQ METHOD™

Your Cyber Quotient — The Intelligence That Now Determines Whether All The Others Matter.

"IQ tells you how smart you are.
EQ tells you how human you are.
Your CQ — your Cyber Quotient —
tells you whether you'll survive the next decade."

- Former CIA Hacker — 8+ Years Inside the Agency
- Appointed by President Obama — Commissioner of Cybersecurity
- Information Security Hall of Fame Inductee
- WSJ #1 Bestselling Author — Cyber Crisis
- Trusted Advisor: Bill Gates · Pentagon · Fortune 500 CEOs

WHAT IS CYBER QUOTIENT?

We measure intelligence. We measure emotional awareness. We have frameworks for social intelligence, adaptability, and leadership.

But the digital world — where every major decision in your life now happens — has never had its own intelligence framework.

Until now.

The CQ Method™ is the first framework to measure and develop Cyber Quotient: your ability to navigate, protect yourself in, and thrive inside the digital world.

It's not a cybersecurity course.
It's not a list of tips.
It's a complete intelligence system —
five levels that raise your ability to think like
the people who built the threats you're facing.

THE INTELLIGENCE STACK

IQ	**Intelligence Quotient** How you process information and solve problems
EQ	**Emotional Quotient** How you understand and manage emotions
SQ	**Social Intelligence** How you navigate relationships and social contexts
AQ	**Adaptability Quotient** How you respond to change and uncertainty
CQ™	**Cyber Quotient** How you survive and thrive in the digital world. The intelligence that now determines whether all the others matter.

THE 5 LEVELS OF CQ™

1 BLINDSPOT

0–24%

"You don't know what you have — or that it's already gone."

Most of America lives here. At CQ Level 1, you don't know what data you have, who can see it, or whether someone is already inside your accounts. The question isn't whether you've been breached. The question is whether you'd know.

2 EXPOSURE

25–44%

"You start to see the open doors — and there are more than you thought."

Awareness begins. You understand your attack surface — phone, laptop, cloud, social. Every default-off security setting. Every app tracking your location 24 hours a day. Level 2 is when you stop seeing social media as connection and start seeing it as a surveillance system.

3 OWNERSHIP

45–64%

"The most dangerous truth: your digital life isn't yours."

Who legally owns your social posts? Your AI-generated work? Your ideas in cloud tools? The answer is almost never you. The Constitution was written for pen and paper. It has never been updated for the digital world. This is the floor-moving moment.

4 LOCK

65–84%

"The embarrassingly simple fixes that close most of your exposure."

Five minutes. A few clicks. Enable 2FA. Switch social to private. Turn off location tracking. The same companies that turned your security off made it just as easy to turn back on. Most risk disappears here. Most people never get here because nobody showed them the door.

5 SENTINEL

85–100%

"You don't just protect yourself. You watch. This is the state of permanent awareness."

Not perfect security — that doesn't exist. But a CQ high enough that you are no longer the easiest target. A Sentinel thinks adversarially by instinct. Before posting: who could use this? Before clicking: who benefits? You are no longer reactive. You are watching. This is the CIA mindset. Once

WHAT NOBODY ELSE IS TEACHING

01

The Default Settings Are A Trap

Google. Amazon. Facebook. Instagram. Apple. Every major platform has robust security built in — and every single one ships with it turned OFF. Not because they forgot. Because your data is the product. And the moment you turn protection

WHY THIS IS OWNABLE:

No other cybersecurity expert indicts the platforms directly and says this was intentional. Everyone else blames the hackers. The CQ Method blames the system

02

You Don't Own Your Digital Life

Anything you post on social media. Anything you put into an AI tool. Any idea, business plan, or creative work you create online — by current law, the platform owns it. Our laws were written for pen and paper. They were never updated for

WHY THIS IS OWNABLE:

This is a legal-political argument about digital rights, not a security tip. It positions the CQ Method at the intersection of cybersecurity, law, AI

03

The Real Threat Is Your Behavior

You would never let a stranger photograph your family, follow your location, or listen to your conversations. But every day on social media, you do exactly that — voluntarily. The threat is not coming from a mysterious dark room.

WHY THIS IS OWNABLE:

This is the mirror-moment that makes audiences uncomfortable in the best possible way. It transforms the conversation from 'watch out for hackers' to 'look at

WHAT'S YOUR CQ?

15 questions. 5 minutes.
A personalized result that tells you exactly where you stand
— and exactly what to do next.

TAKE THE FREE CQ ASSESSMENT
drericcole.org/CQ

01	02	03	04	05
BLINDSPOT	**EXPOSURE**	**OWNERSHIP**	**LOCK**	**SENTINEL**
0–24%	25–44%	45–64%	65–84%	85–100%
You don't know what you have — or that it's already gone.	You're starting to see the open doors.	The most dangerous truth: your digital life isn't yours.	Most of your doors are closed. Now close the rest.	Permanent awareness. You watch. You think like the attacker.

Former CIA Hacker · Presidential Cyber Commissioner · WSJ #1 Bestselling Author
Advisor to Bill Gates, the Pentagon, and Fortune 500 CEOs