# Profit-Centric Cybersecurity Is Great for Today's Companies

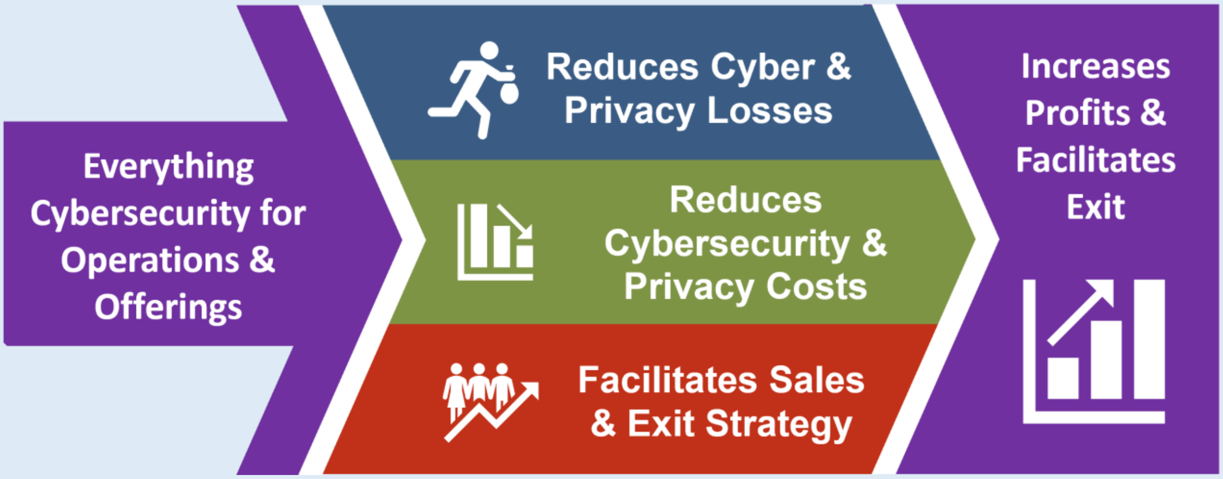
## THE CYBERSECURITY PARADOX

Today's companies embody innovation, using transformative approaches to disrupt markets and change the world. They face significant, rapidly growing cyber risks. And suffering even one cyber-attack can be devastating, announcing to the world that they and their offerings are untrustworthy.

Yet, despite impressive innovative abilities and scary cyber risks, many companies settle for a deficient, traditional "cybersecurity" approach that has (1) repeatedly failed to prevent devastating cyber-attacks, (2) often leaves the company overly dependent on a single point of failure (e.g., a traditional CISO), and (3) fails to help develop the cybersecurity and privacy proof needed to increase sales and facilitate the best exits.

The solution is Profit-Centric Cybersecurity: a low risk, commonsense innovation that eclipses the deficient, traditional approach to cybersecurity.

### PROFIT-CENTRIC CYBERSECURITY



Everything Cybersecurity for Operations & Offerings

Reduces Cyber & Privacy Losses

Reduces Cybersecurity & Privacy Costs

Facilitates Sales & Exit Strategy

Increases Profits & Facilitates Exit

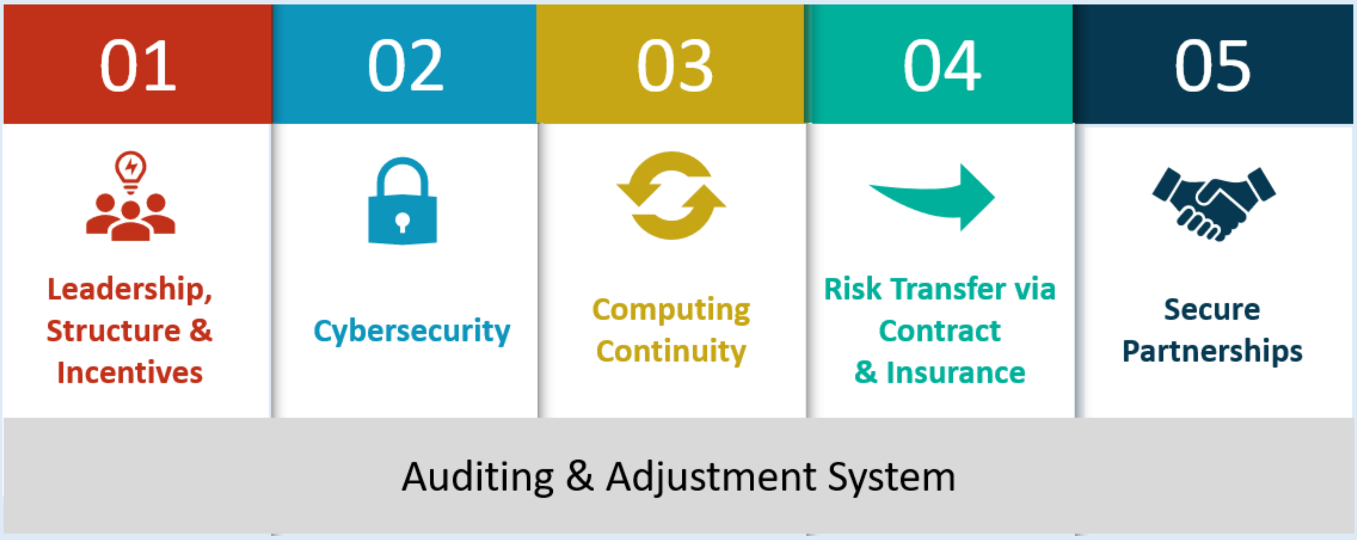
## HOW THE TRADITIONAL APPROACH IS DEFICIENT

The traditional "cybersecurity" approach focuses on using technologies, people, and processes to protect your computing operations and digital data from attack. It often involves suboptimal deference by leadership to technologists who don't have all the multidisciplinary expertise to properly protect the company from the devasting cyber risks explained here.

This deference often leads to what we call the CISO Deficiency, which increases your vulnerabilities and overall mitigation costs; as well as impedes valuable contributions from non-technologists such as financial professionals, risk managers, and in-house counsel. One danger is the technology-centric incident response plan adopted by most companies. As this article explains, traditional incident response plans suffer from a slew of preventable deficiencies that leave you ill-prepared to mitigate the devastating harm from cyber-attacks.

# WHY PROFIT-CENTRIC CYBERSECURITY IS BETTER

**1. Fully Leverages The Five Mitigation Tools:** Cybersecurity is just one of the five cyber risk mitigation tools that companies should use:



01 Leadership, Structure & Incentives

02 Cybersecurity

03 Computing Continuity

04 Risk Transfer via Contract & Insurance

05 Secure Partnerships

Auditing & Adjustment System

**Leadership, structure, and incentives:** The right leadership, organizational structure and incentives make all the other techniques more effective.

**Cybersecurity:** It comprises the technologies, people, and processes used to protect your computing operations and digital data from attack.

**Computing continuity:** It comprises the technologies, people, and processes that restore your computing operations and digital data after an attack.

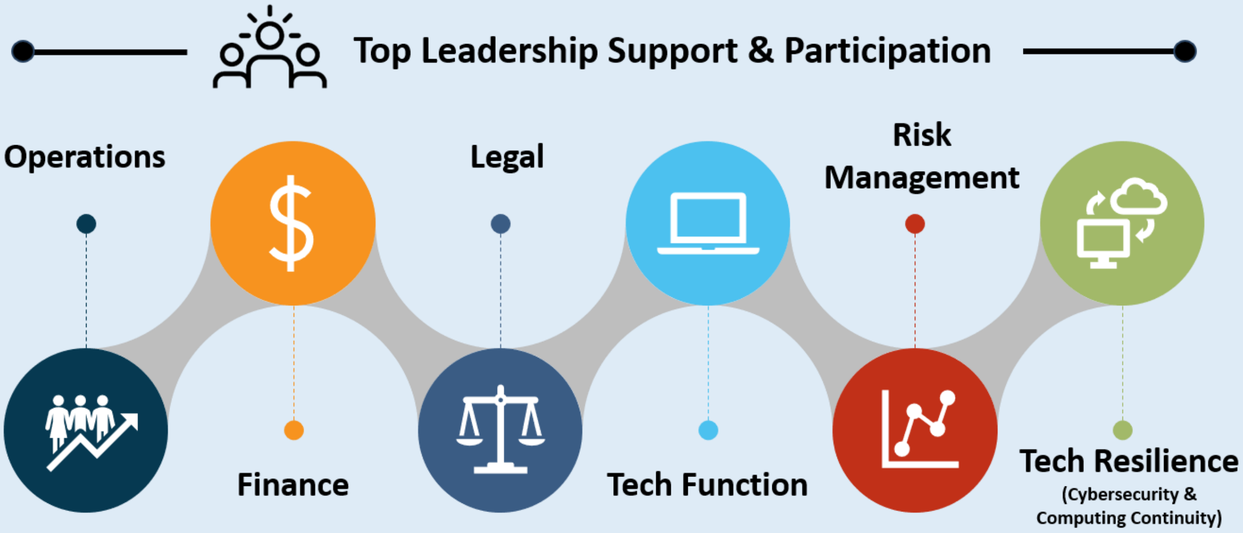
**Risk transfer:** It involves using contract and/or insurance to transfer cyber risks to other companies.

**Secure partnerships:** This means ensuring that critical partners have sufficient cybersecurity and/or computing continuity to protect your operations.

An "Auditing and Adjustment System" is vital to success. The best approach to cyber risk mitigation focuses on creating auditable, customized checklists for all your organization's multi-tool mitigation efforts. While the billion-dollar Equifax breach is the poster child for the importance of auditing, deficient auditing was a major contributor to almost every major cyber-attack in history.

**POWERFUL TIP:** Using the term "cybersecurity" to organize your efforts to mitigate cyber risks often undermines the true job to be done – namely, the cost-effective (1) mitigation of the devastating harm that cyber-attacks can inflict on your company and (2) creation and use of cybersecurity and privacy marketing materials that increase sales and facilitates profitable exits. Change it to Profit-Centric Cybersecurity for better results.

**2. Deploys a Multidisciplinary Team:** To effectively use the 5 mitigation tools, your company will need top leadership support for – and participation in – a cohesive team covering these disciplines:


Top Leadership Support & Participation
Operations
Finance
Legal
Tech Function
Risk Management
Tech Resilience
(Cybersecurity & Computing Continuity)

Each discipline plays an important role in cost-effectively mitigating your cyber risks. Unfortunately, too many traditional CISOs lack the expertise and skills needed to create and effectively lead these teams – which is part of [the CISO Deficiency].

**3. Increases Profits & Facilitates Exits:** When customers and prospects doubt your company's cybersecurity and privacy, you can lose sales. During an exit, your buyers will scrutinize your security and privacy. Therefore, today's companies must be able to prove their cybersecurity and privacy in ways that promote confidence, close more sales, and facilitate profitable exits. This is a big part of Practical Cyber's profit-centric approach.

## HOW WE HELP COMPANIES USE OUR APPROACH

**Works With or Without a CISO:** You can use Profit-Centric Cybersecurity with or with a CISO. It is less expensive without one. But good CISOs embrace it because (1) it makes them more effective and (2) they support that it institutionalizes the knowledge, expertise, and processes essential to cost-effectively mitigate your cyber risks. Smart C-Suites embrace our approach because it simultaneously improves overall cyber risk mitigation, avoids the CISO Deficiency, and facilitates sales and exits.

**Step 1 – Identify Your Risk Tolerance & Internal Capabilities:** Step 1 has two parts: (1) help you identify your unique risks and risk tolerance and (2) evaluate your internal capabilities to deploy our approach. This allows Practical Cyber and you to determine the best allocation of responsibilities.

**Step 2 – Set & Implement a Customized Cost-effective System:** The second step is to set and then implement a customized, cost-effective system that simultaneously protects you from cyber-attack, reduces your mitigation costs, and helps you prove your cybersecurity and privacy in ways that sell more of your offerings and facilitate your exit.

# Our Multidisciplinary Core Team

We are a **multidisciplinary** cyber and privacy risk mitigation firm driven by the cost-effective integration of these three proven, top-flight experts:

### Cybersecurity & Computing Continuity Expert – Dr. Marc Rogers.

Internationally known cybersecurity expert and founder of MKR Forensics.

Tenured Cybersecurity Professor and Executive Director of the graduate and undergraduate cybersecurity programs at one of the top university cybersecurity departments in the world.

25+ years practical cybersecurity experience enhanced by academic career & access to talented graduate students (e.g., Alissa Gilbert) and alumni with excellent practical experience.

### Cyber & Privacy Law + Cyber Risk Transfer Expert – Elliot Turrini, JD.

Former federal cybercrime prosecutor, cyberlaw/privacy attorney in private practice, & tech company General Counsel.

Cyber risk mitigation & risk transfer expert – both insurance and contract.

Co-Editor & Author of Cybercrimes: A Multidisciplinary Analysis.

### Cybersecurity Researcher, Practitioner, & Pragmatist – Alissa Gilbert Ph.D. Candidate.

Nationally ranked ethical hacker. Highly skilled vulnerability tester.

One of the top cybersecurity researchers in the United States. Many years of practical experience protecting organizations from cyber-attack

COO of CircleCityCon, an elite cybersecurity conference.

Ph.D. candidate and instructor at Purdue University.