



HOW PRACTICAL CYBER HELPS CLIENTS REDUCE THEIR CYBERSECURITY COSTS

Many companies are significantly overspending on cybersecurity. The main problem is that the cybersecurity industry has found clever ways to use fear, uncertainty, doubt, and information asymmetries to over-charge.

Practical Cyber empowers its clients to avoid being taken advantage of and exploited.

INTRODUCTION

This article solely focuses on how Practical Cyber reduces what its clients pay for cybersecurity. It does not detail how and why Practical Cyber's services are more effective and cost less.

HOW WE REDUCE YOUR CYBERSECURITY COSTS

Cybersecurity is one of [the 5 cyber risk mitigation tools](#), and it comprises the technologies, people, and processes used to protect your computing operations and digital data from attack. In general, your cybersecurity costs come from the following categories:

- **Technologies:** These include things like firewalls, antimalware software, SIEMs, intrusion prevention systems, and many more.
- **People:** This refers to the people you hire to defend against cyber-attack such as a CISO and people who perform specific security functions.
- **Processes & policies:** This refers to processes like your [Cyber Incident Mitigation Protocols](#) and policies like an acceptable use policy -- which need to be in place continuously.
- **Training:** This includes training for employees and cybersecurity personnel.
- **Cyber insurance:** The cost of cyber liability insurance is rapidly rising.

Here's how Practical Cyber helps you reduce the costs in each of these aforementioned general categories.

Technologies: As Appendix A explains, every company must properly and continuously implement a foundational set of cybersecurity technologies and processes. But, far too many companies are over-paying for cybersecurity because they have bought the wrong technologies and/or unnecessary ones. For example, if your company uses Google Workspace Enterprise Edition, it can leverage Google's advanced security tools (e.g., endpoint management) to save a

People: In many situations, the biggest cybersecurity over-spending is on a full-time CISO. As [this article explains](#), most companies are better off without a traditional CISO – assuming they engage a multidisciplinary, multi-tool team like Practical Cyber. In these situations, Practical Cyber can immediately save your company over \$100K per year just by not hiring a CISO.

Processes & Policies: The major cost is creating and maintaining effective ones. Most companies have a mixed bag of procedures and policies that were created and modified by different people. This leads to less effective, overlapping policies and suboptimal procedures. Practical Cyber excels at helping its client create clear, effective, and enduring processes and policies – particularly [Cyber Incident Mitigation Protocols](#), which are far more effective than traditional incident response plans.

Training: Of the cybersecurity “cost” categories, training should be the easiest to deploy cost-effectively. There are a few good cybersecurity training companies that you should consider. We help our clients pick the best one for their needs, as well as provide customized training for their cybersecurity personnel.

Cyber Insurance: How you shop for cyber liability insurance and your cybersecurity controls can substantially influence the cost and the overall value of your coverage. These policies are tedious to read and difficult to understand, requiring multidisciplinary expertise that few companies other than Practical Cyber possess. Therefore, Practical Cyber can simultaneously help you pick the right policy and maximize its coverage.

PRACTICAL CYBER’S MULTIDISCIPLINARY TEAM

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 and alumni with excellent practical experience.

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



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

Cyber risk mitigation & 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.

To learn more, email Elliot Turrini at Elliot@PracticalCyber.com.