PRACTICAL CYBER'S ENHANCED EXTERNAL CISO SERVICE

More Effective than a Traditional Chief Information Security Officer for Less Money

01 HOW IT WORKS

MULTDISCIPLINARY EXPERTISE

To protect you from cyber-attacks and facilitate sales, our Enhanced External CISO Service integrates the 3 most valuable areas of expertise:

(1) **Chief Information Security Officer:** Helps you protect your computing operations from cyber-attack.

(2) **Cyber & Privacy Law:** Helps you (a) comply with all cybersecurity and privacy regulations and (b) properly use contract and insurance to transfer cyber risk to other parties.

(3) **Cyber Opportunity Expert:** Helps you close sales by proving your cybersecurity to customers and partners.

CUSTOMIZED TO YOUR CYBER RISKS, NEEDS & PERSONNEL

YOUR CYBER RISKS & NEEDS

OPERATIONAL INTERRUPTIONS	Cyber-attacks (e.g., ransomware) & human errors (e.g., improper configurations) can interfere with your operations.
PRODUCT MALFUNCTIONS	Cyber-attacks & human error can cause product malfunctions that harm customers and partners.
DATA BREACHES	Data breaches now cost millions. The problem is worsening because there's more personal information and privacy laws are stricter.
IP & FINANCIAL THEFT	Cyber-attacks can steal your organization's money and/or IP such as trade secrets.
COMPLIANCE & SALES ISSUES	To generate revenue, many companies must prove their cybersecurity to customers, partners, and/or regulators.

OUR CUSTOMIZATION PROCESS

We customize our Enhanced External CISO Service to your unique cyber risks, needs and personnel. So you only pay for what you need to mitigate your cyber risks and leverage your cyber opportunities.

The main influences on customization include your:

(1) use of computing technologies,

(2) existing cyber risk mitigation & opportunity efforts,

(3) personnel, and

(4) regulatory obligations.

This approach yields greater overall efficacy, lower costs, and a stronger, more self-sufficient internal team.

OUR SERVICES: When customizing our services we select from all these options.

Info@PracticalCyber.com -- www.PracticalCyber.Com

02 COSTS LESS

TRADITIONAL VERSUS PRACTICAL CYBER

YOUR PRACTICAL CYBER COSTS = LESS THAN $120K

STEP 1 – A CUSTOM CYBER RISK MITIGATION & OPPORTUNITY PLAN

WHAT HAPPENS: After evaluating your unique cyber risks and needs, we propose a fixed-price, customized and comprehensive cyber risk mitigation & opportunity plan that best leverages your existing resources and efforts.

COST EST. $8-30K: The exact cost depends on your use of computing technologies, cyber risk mitigation efforts, personnel, regulatory needs, and cybersecurity documentation.

STEP 2 – HELP IMPLEMENTING AND EXECUTING YOUR PLAN

WHAT HAPPENS: We help you cost-effectively implement and execute your plan. The goal is to make you as self-sufficient as you desire. And, these exact services depend on your needs.

COST EST. $10-40K: The cost depends on the services you need us to provide. No two organizations need the same services; each has a unique situation,

STEP 3 – ONGOING ASSISTANCE

WHAT HAPPENS: After your plan is implemented and executed properly, we can help ensure that you adjust it as needed. This ongoing assistance can include many different aspects.

COST EST. $10-50K: The exact cost depends on the ongoing support services you need. Each organizations has unique needs; and you only pay for vital ongoing assistance.

OUR CORE VALUES: ALLIGNED INTERESTS & NO UP-SELL

Cyber risk mitigation is filled with information asymmetries that can lead to over-spending and/or the wrong mitigation techniques. To avoid such waste and align our interests with yours, we do the following: (1) only recommend the bare essential mitigation techniques, and for each recommendation explain its cost-effectiveness; (2) only recommend the most effective technologies and never take any compensation from the vendors; and (3) avoid the typical consulting upsell business model, preferring annual fixed price arrangements that overtly quantify the value we deliver.

03 WHO IS PRACTICAL CYBER?

We are driven by the cost-effective integration of these two experts:

Cybersecurity Expert – Purdue University's Dr. Marc Rogers

Internationally known cybersecurity expert and founder of MKR Forensics.

Executive Director Purdue Cybersecurity Programs (one of the top programs in the nation).

25+ years practical cybersecurity experience enhanced by academic career.

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

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

Cyber risk mitigation & transfer expert.

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

OUR SERVICES: Our services include all these options.

04 HOW TO GET STARTED

OPTION 1 – EMAIL US TO GET THE BALL ROLLING: Info@PracticalCyber.com

OPTION 2 – HIGH-LEVEL CYBER RISK MITIGATION & OPPORTUNITY PLAN

WHAT HAPPENS: After evaluating your unique cyber risks and needs, we provide a customized and comprehensive cyber risk mitigation & opportunity plan that best leverages your existing resources and efforts.

COST EST. $8-30K: The exact cost depends on your use of computing technologies, cyber risk mitigation efforts, personnel, regulatory needs, and cybersecurity documentation.

OPTION 3 – TRY ONE OF OUR QUICK STARTS

1. C-Level Sanity Check
2. Board of Directors Consultation
3. Technological Intro to Revenue-Centric Cybersecurity

For the details, use our website's Quick Starts page.

05 SUMMARY OF OUR SERVICES (part 1)

Practical Cyber can help your organization in many ways. Drawing from the following options, we customize how we help your organization mitigate its cyber risks:

CYBERSECURITY & PRIVACY IMPROVEMENTS: We can help improve all aspects of your cybersecurity & privacy protections – (1) technologies (e.g. firewalls, anti-virus, EDRs, SIEMs, data encryption); (2) people (e.g. info security professionals, cyber lawyer, risk managers); (3) policies and processes (e.g. cyber incident response plan, training, compliance, security policies); and (4) training (e.g., employee cybersecurity training, professional development for your cyber risk mitigation personnel, cyber-attack simulation training).

COMPUTING CONTINUITY EFFICACY: Computing Continuity refers to your ability to fully restore all computing operations after a cyber-attack. Cyber-attacks that interfere with your business operations are almost inevitable – particularly because of the rapidly growing ransomware threats. This makes computing continuity critical. Because we have found that some organizations have not properly set up and/or tested their Computing Continuity, we include this option in our services.

CYBERSECURITY ENDORSEMENTS: There are times when an organization needs a cybersecurity expert to provide an endorsement about the strength of its cybersecurity. This need can arise with customers, partners, vendors, and/or strategic buyers. We provide effective, objectively valid cybersecurity endorsements.

PREPARATION OF INCIDENT MITIGATION PROTOCOLS: A critical part of cyber risk mitigation is effectively responding to cyber incidents, which can literally save millions. To do so, you need to prepare and practice a customized Incident Mitigation System, which are more effective than traditional incident response plans. We can help you create and deploy this type of system.

PROFESSIONAL DEVELOPMENT FOR STAFF: We can help your cybersecurity staff develop professionally. We provide customized development plans for each person. Because Dr. Rogers has been a preeminent cybersecurity professor, his mentoring delivers substantial value.

IMPROVE YOUR CONTRACTUAL MITIGATION: Companies often share cyber risk with their customers, vendors, and partners. The right contractual provisions are critical for transferring shared cyber risks. While your lawyers have the general contracting expertise that is part of what's need to succeed in this area, some will benefit from our cyber risk expertise. We, therefore, can help you use contract to mitigate your cyber risks.

IMPROVE YOUR INSURANCE MITIGATION: Using insurance to mitigate cyber risks can be effective but terribly complex. But, some organizations lack the time and expertise needed to conduct a proper "gap analysis" for cyber risks, and simply rely on an insurance broker. That can lead to material problems and high-costs. With Practical Cyber's help, your legal and risk-management resources can materially improve your ability to use insurance to better mitigation cyber risks.

ORGANIZATIONAL ADJUSTMENTS: Even small adjustments to your leadership, structure and incentives can materially improve the efficacy of your cyber risk mitigation. This is particularly true for Boards of Directors, which is one of our specialties.

05 SUMMARY OF OUR SERVICES (part 2)

SET & EXECUTE AN ANNUAL SCHEDULE ORGANIZED BY THIS CYCLE: We can help you create a detailed annual schedule organized around this Cyber Risk Mitigation Cycle:

1. QUANTIFY RISKS & OPPORTUNITIES

- Set & deploy a Multidisciplinary Team.
- Assess & quantify your Unique Cyber Risks & Opportunities.

2. SET CYBER RISK MITIGATION & OPPORTUNITY PLAN

- Create a 2-Part Cyber Risk Mitigation System with Auditing & Adjustment.
- Allocate Resources among the 5 Mitigation Tools.

4. AUDIT & ADJUST

- Effectively implement your auditing system.
- Adjust your Cyber Risk Mitigation & Opportunity Plan as needed.

3. EXECUTE THE PLAN

- Implement your Cyber Risk Mitigation & Opportunity Plan.
- Use customized Cyber Incident Mitigation Protocols, not a typical incident response plan.

Efficiently executing this schedule is critical to success. And, it helps your organization establish and maintain the type of candid, consistent and rapid communication needed for an effective Cyber Risk Mitigation System.

ASSESSMENT OF AUDITING EFFICACY: Auditing is a critical (often improperly implemented) aspect of cyber risk mitigation. One common reason is that many organizations have trouble analyzing the efficacy of their own operations because it is difficult enough to execute the strategy without having to audit it. We, therefore, can help you assess the efficacy of your auditing system for cyber risk mitigation in ways that (1) identify and rectify deficiencies and (2) prevent your organization from suffering preventable losses due to cyber-attack. For an illustration of the power of auditing, consider reading the Equifax story in Appendix C.

ASSISTANCE TO THE BOARD OF DIRECTORS: In some instances, companies will benefit from Practical Cyber talking with their boards. This assistance can help the board (1) appreciate the benefits of cyber risk mitigation and (2) more proactively and effectively execute its cyber risk mitigation oversight responsibility.