PRACTICAL CYBER'S POWERFUL CYBERSECURITY INNOVATION

A DETAILED SUMMARY OF OUR MULTI-TOOL, MULTIDISCIPLINARY CYBER RISK MITIGATION APPROACH

ALL OUR SERVICES SPRING FROM OUR MULTI-TOOL, MULTIDISCIPLINARY CYBER RISK MITIGATION INNOVATION

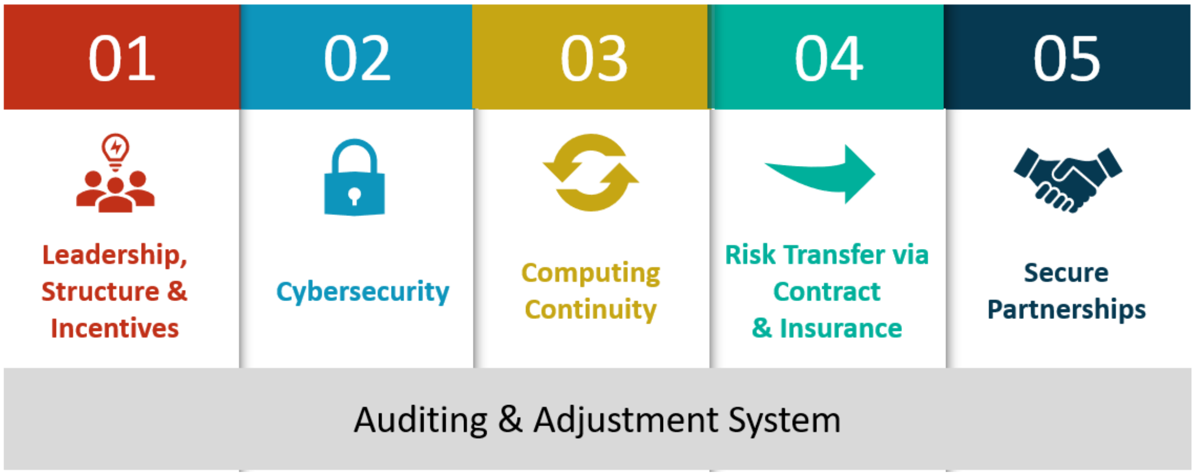
All our methods and services spring from our innovative multi-tool, multidisciplinary cyber risk mitigation approach explained herein. Our website summarizes our services.

WHY MULTI-TOOL, MULTIDISCIPLINARY CYBER RISK MITIGATION IS BETTER THAN TRADITIONAL CYBERSECURITY

An organization's main "cybersecurity" goal should be to develop and maintain a cost-effective system to mitigate the harm from its 3 main cyber & privacy risks:

1. Operational interruptions – An example is the June 1, 2020 ransomware attack on the University of California, San Francisco that encrypted data in its School of Medicine for which the institution paid a $1.14 million ransom. A reputable cybersecurity company reported that in 2019 alone, 89 U.S. universities, colleges, and school districts were victimized by ransomware.
2. Data breaches – Examples include the 1.27 million records stolen from Georgia Tech in 2019 when a central database was hacked and the 1.12 million records stolen from Washington State University in 2019 when criminals stole a hard drive backup. The Ponemon Institute's well-respected report stated that the average data breach in 2019 cost $3.92 million.
3. IP & financial theft – This includes the types of intellectual property theft by foreign government-sponsored attackers about which the FBI in 2019 and 2020 has warned universities and colleges. Because of their scientific/medical research, academic institutions are prime targets for economic espionage; and cyber-attack is one of the main theft techniques.

Unfortunately, using the term "cybersecurity" to organize how your organization achieves this goal can both leave it unnecessarily vulnerable to cyber-attack and inflate its costs. The solution is to find a cost-effective, customized mix of these five cyber risk mitigation tools:



01 Leadership, Structure & Incentives

02 Cybersecurity

03 Computing Continuity

04 Risk Transfer via Contract & Insurance

05 Secure Partnerships

Auditing & Adjustment System

Leadership, structure & 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.

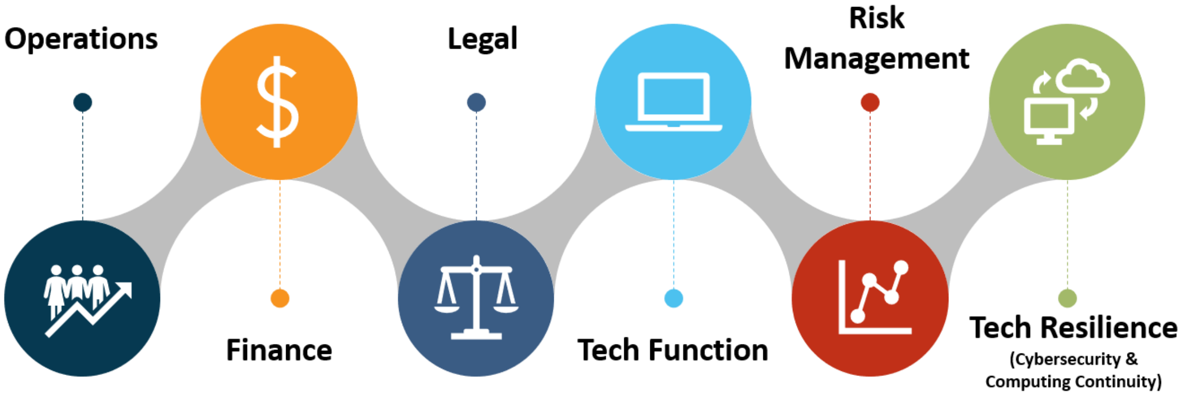
Computing continuity: It comprises the technologies, people, and processes that restore your computing operations and digital data after an attack.

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.

YOU NEED A MULTIDISCIPLINARY TEAM

A multidisciplinary team is needed to properly leverage the 5 mitigation tools. Your team should include the following disciplines:



Each discipline plays an important role in cost-effectively mitigate your cyber and privacy risks. Unfortunately, too many traditional CISOs lack the expertise and skills needed to create and effectively lead these teams.

HOW WE HELP ORGANIZATIONS UPGRADE TO OUR INNOVATIVE APPROACH

A. Identify Risk Tolerance & Staff Capabilities: The first step is helping each organization identify its unique risk tolerance, and for Practical Cyber to evaluate the school's internal capabilities to deploy a multidisciplinary approach. This will allow Practical Cyber and the school to determine the extent to which each organization will apply each of the 5 mitigation tools in its cyber risk mitigation system; as well as how many of the multidisciplinary team roles Practical Cyber should play.

B. Improvement Roadmaps: For most organizations, Practical Cyber will create cybersecurity and computing continuity improvement roadmaps. We recommend improvement roadmaps for all five mitigation tools, though.

C. Implement Improvements: Organizations decide which improvements to implement themselves because, in many instances, they can efficiently make the improvements. There might be situations when it is more efficient for Practical Cyber to implement an improvement. When that occurs, Practical Cyber will provide the organization a proposal including a price and alternatives.

D. Create Customized Cyber Incident Mitigation Protocols: Most likely, your organization already has some form of traditional incident response plan. From experience, Practical Cyber has learned that after an organization adopts multi-tool, multidisciplinary cyber risk mitigation, it is more efficient to create new Cyber Incident Mitigation Protocols than recommend changes to an existing incident response plan. Our innovative Cyber Incident Mitigation Protocols are far more effective than traditional incident response plans. To learn more, visit our website.

E. Create Customized, Auditable Checklists: The best approach to cyber risk mitigation focuses on creating auditable, customized checklists for all your organization's multi-tool mitigation efforts – each specifying timelines and responsible parties. Therefore, when helping an organization adopt multi-tool, multidisciplinary cyber risk mitigation, Practical Cyber helps it create customized auditable checklists for all its mitigation efforts. Here is a summary of Practical Cyber's methodology for creating auditable checklists:

- Identify every aspect of each mitigation effort.
- Document what must be done for each aspect – including timing such as daily, weekly, monthly, annually.
- Identify who is responsible for each aspect.
- Identify and/or develop a system to audit whether each aspect has been properly and timely implemented. This includes identifying the details of how the audit will be done, the timing, and who is responsible.

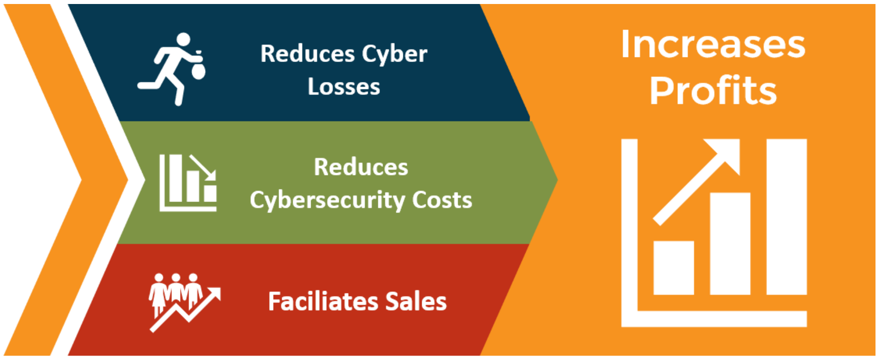
F. Create Process/Checklist for Securely Adding New Computing Technologies: Practical Cyber helps each organization create a process/checklist for securely adding new computing technologies into its operations. This will include vetting the cyber and privacy risks of any new computing technology, as well as creating a mitigation strategy to be incorporated into the organization's auditable checklists.

OUR APPROACH HELPS INCREASE YOUR PROFITS

THREE PROFIT TOOLS

As the graphic to the right shows, our approach empowers Practical Cyber to help increase your profits in three inter-connected ways.

The following explains each:



Reduces Cyber Losses

Reduces Cybersecurity Costs

Faciliates Sales

Increases Profits

i. REDUCES CYBER LOSSES

Cyber losses arise when a cyber-attack harms (a) your operations or offerings or (b) the operations or offerings of one of your critical vendors or partners.

Our Multi-tool, Multidisciplinary Approach empowers us to reduce your true out-of-pocket losses from cyber-attack far more effectively than the traditional approach.

ii. REDUCES CYBERSECURITY COSTS

TRADITIONAL

Full-time CISO = $236K
+
External Cyber & Privacy Lawyer = $50K
+
External Cyber Risk Expert = $35K

= $321K per year

VERSUS

PRACTICAL CYBER

<$125K per year =

External CISO
+
External Cyber & Privacy Lawyer
+
External Cyber Opportunity Expert

iii. HELPS SALES & PARTNERSHIPS

To close enough sales in today's intensely computer-dependent economy, most companies must (to some degree) show customers and/partners that they and their offerings are cybersecure. But, many companies vastly overspend when trying this and/or fail to produce high-quality "cybersecurity" sales materials.

Practical Cyber makes sure that you know the type of cybersecurity that your customers and/or partners want to see; and, then we produce high-quality, customized cybersecurity sales materials customized to your situation.

Your Effective Cybersecurity White Paper

PRACTICAL CYBER: MULTIDISICIPLINARY EXPERTS

We are a multidisciplinary cyber and privacy risk mitigation firm driven by the cost-effective integration of these two 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 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.

Use our website to learn about our services.

HOW TO GET STARTED

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

OPTION 2 – TRY ONE OF OUR QUICK STARTS

1. C-Level Sanity Check
2. Board of Directors Consultation
3. Intro to Multi-tool, Multidisciplinary Cyber Risk Mitigation

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