PRACTICAL CYBER'S FIVE CYBER RISK MITIGATION TOOLS EXPLAINED

Properly Allocating Your Resources Among the Five Tools Is Vital to Cost-Effectively Protect Against the Harm from Cyber-Attacks

INTRODUCTION TO THE 5 CYBER RISK MITIGATION TOOLS

Traditional cybersecurity – i.e., the technologies, people, and processes used to prevent and mitigate cyber-attacks – is just one of the five tools that your organization should consider for mitigating its unique cyber risks. The following infographic introduces the 5 Cyber Risk Mitigation Tools and the fact that you need an auditing and adjustment system covering all your mitigation efforts.

LEADERSHIP, STRUCTURE & INCENTIVES: The right leadership, organizational structure and incentives are critical to effective cyber risk mitigation but difficult to implement. They make all the other techniques more effective.

CYBERSECURITY: Involves all efforts to prevent and limit unauthorized access, use, and/or interference with your computing devices (i.e., any device using a CPU and/or IP address such as computers, mobile devices, connected devices like printers, and IoT devices), software, and digital data.

COMPUTING CONTINUITY: The technologies, people, and processes that restore your computing operations to their original operational state after a harmful cyber-incident

RISK TRANSFER: Involves using contract and/or insurance to mitigate and transfer cyber risks shared with customers, vendors, and partners.

SECURE PARTNERSHIPS: Involves proactively ensuring that your critical partners have sufficient cybersecurity so that their cyber-incidents don't unduly interfere with your operations.

AUDITING & ADJUSTMENT SYSTEM: A critical part of Revenue-Centric Cybersecurity is auditing that you've properly implemented your Cyber Risk Mitigation and Opportunity Plan. Auditing should include finding improvements and helping you make the proper adjustments to all your efforts.

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