PRACTICAL CYBER'S 4-PART CYBER RISK MITIGATION CYCLE

THE 4-PART CYCLE IS THE KEY TO USING REVENUE-CENTRIC CYBERSECURITY

HOW IT WORKS

The key to leveraging Revenue-Centric Cybersecurity is to properly and continuously deploy the 4-Part Cyber Risk Mitigation Cycle summarized in the graphic below. This Cycle efficiently organizes how to cost-effectively mitigate your unique cyber risks and develop the cybersecurity proof to best drive revenue.

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.

TIPS FOR THIS CYCLE

1. Use the right Multidisciplinary Team. See Page 2.
2. Part 2's "Cyber Risk Mitigation & Opportunity Plan" should show how you will allocate resources among the 5 Cyber Risk Mitigation Tools (see Page 3) and specify how you will audit and adjust all your efforts.
3. Part 3 "Execute the Plan" focuses on implementing your plan.
4. Part 4 "Audit & Adjust" focuses on properly auditing and improving your plan.

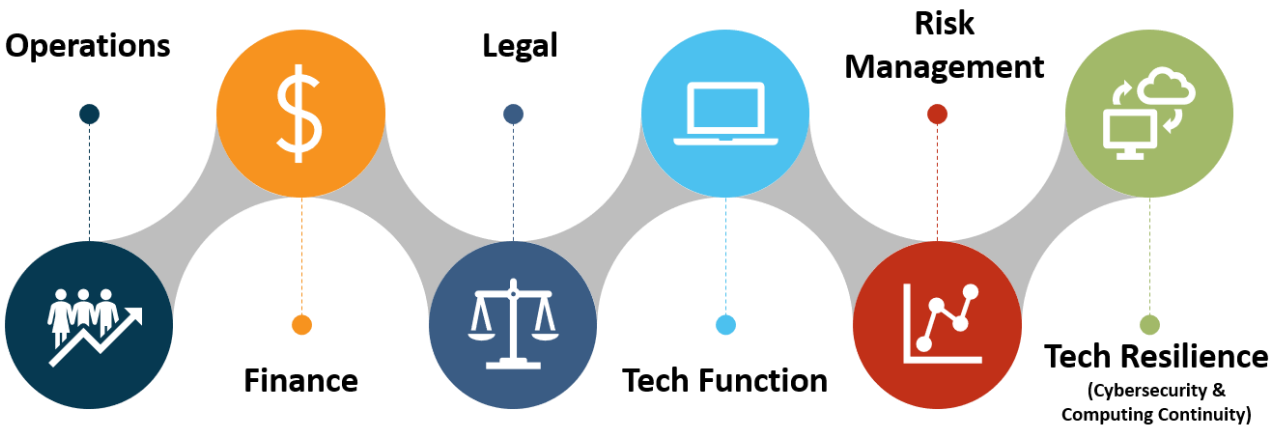
DOWNLOAD A DETAILED SUMMARY OF REVENUE-CENTRIC CYBERSECURITY

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

HOW TO SET & DEPLOY YOUR MULTIDISCIPLINARY TEAM

The right Multidisciplinary Team helps organizations properly implement every aspect of Revenue-Centric Cybersecurity.

Critical parts of creating the right team include assigning the strong leadership, ensuring the leadership has the proper authority and budget, and allowing leadership to create, develop and leverage a multidisciplinary mitigation team covering these areas:



TIPS FOR YOUR TEAM

1. Building the Team: Sometimes you can create a strong Multidisciplinary team by a mix of (1) enhancing the skills of existing team members and (2) using external experts like Practical Cyber to fill gaps.
2. Avoiding Impediments: At times, the requisite internal talent isn't enough because (1) many organizations don't how to properly use Revenue-Centric Cybersecurity, (2) many fail to implement the right leadership and/or goals, and (3) existing corporate structures and traditional cybersecurity and risk-management practices get in the way.
3. Common Organizational Impediments: Some common organizational traits degrade the team's effectiveness: e.g., (1) significant (and sometimes dangerous) deference to technologists, (2) deficient oversight by finance and operations (particularly failure to quantify risks and properly prioritize, allocate, and audit limited mitigation resources), (3) ineffective and unnecessary separation between operational and product cyber risk mitigation, and (4) failure to incorporate an intelligent cyber risk mitigation approach into product design

DOWNLOAD A DETAILED SUMMARY OF REVENUE-CENTRIC CYBERSECURITY

PRACTICAL CYBER'S 4-PART CYBER RISK MITIGATION CYCLE

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 Tools and the fact that you should have 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.

DOWNLOAD A DETAILED SUMMARY OF REVENUE-CENTRIC CYBERSECURITY

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