PRACTICAL CYBER'S INCIDENT MITIGATION PROTOCOLS

WHY OUR CUSTOMIZED CYBER INCIDENT MITIGATION PROTOCOLS ARE BETTER THAN TRADITIONAL INCIDENT RESPONSE PLANS

PROBLEMS WITH TRADITIONAL INCIDENT RESPONSE

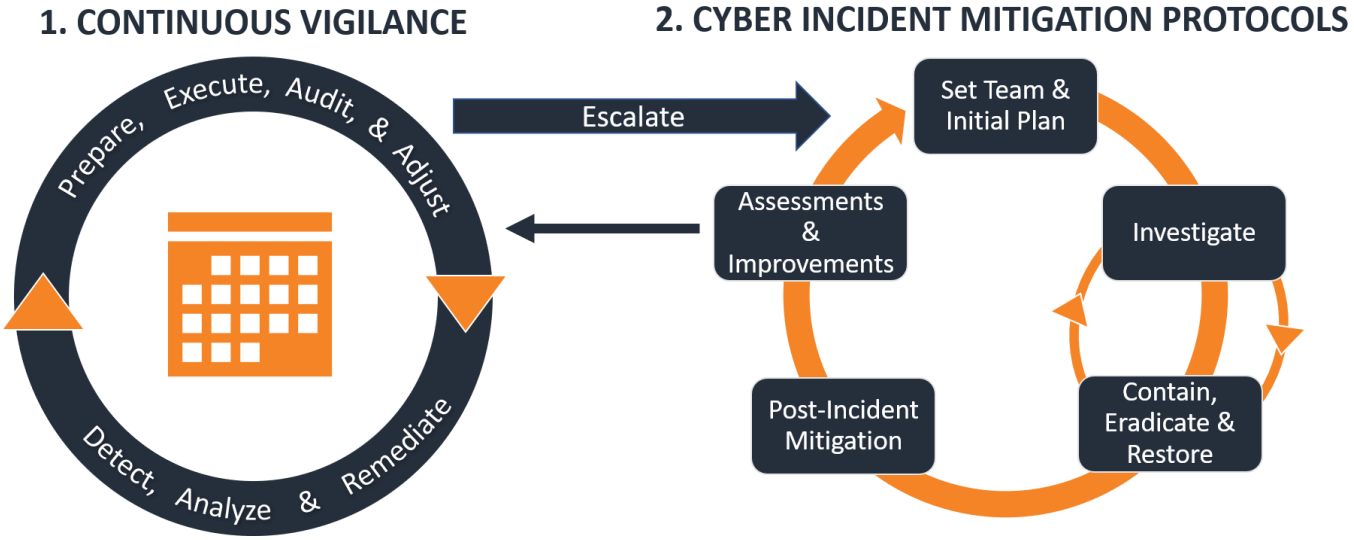
Even organizations with state-of-the-art defenses are vulnerable to today's sophisticated cyber-attacks. All organizations, therefore, should create, test, and regularly update a system that effectively mitigates the harm from cyber-attacks they cannot prevent. This is traditionally referred to as "incident response", and many organizations have some form of traditional incident response plan – often part of a larger business continuity plan.

Unfortunately, traditional cyber incident response plans suffer from a slew of preventable deficiencies – as Appendix A explains. This means that many organizations are ill-prepared to mitigate the harm from the cyber-attacks they cannot prevent.

OUR CYBER INCIDENT MITIGATION PROTOCOLS

Practical Cyber used its experience and its innovative multi-tool, multidisciplinary approach (see Appendix B) to upgrade the traditional incident response plan to more effective Cyber Incident Mitigation Protocols. Organizations can upgrade without adopting multi-tool, multidisciplinary cyber risk mitigation, and upgrading provides the additional benefits explained on page 4.

To upgrade, organizations must understand where their Cyber Incident Mitigation Protocols fit into a two-part cyber risk mitigation system – as this infographic introduces:



Continuous Vigilance: Continuous Vigilance focuses on everything your organization should do to mitigate cyber risks before an exigent incident requires immediate remediation. It includes the following –

Prepare, Execute, Audit, & Adjust: This refers to all your efforts to create, execute, and audit, and adjust your comprehensive cyber risk mitigation.

Detect & Analyze: This comprises the systems, software, and people needed to promptly and efficiently identify, analyze, and classify cyber vulnerabilities and incidents (e.g., cyber-attacks or malfunctions). The goals are (1) to identify vulnerabilities and properly remediate them before they are exploited and inflict harm and (2) to accurately identify and classify incidents, minimize false positives and cost-effectively escalate only material incidents to your Cyber Incident Mitigation Protocols.

Remediate: This includes your ability to restore operations and data after a cyber incident – also known as Computing Continuity, which is one of the 5 tools in multi-tool cyber risk mitigation explained in Appendix B. The recent increase in ransomware attacks heightens your need for effective Computing Continuity.

Escalate: The process for escalating material cyber incidents to your Incident Mitigation Protocols.

Cyber Incident Mitigation Protocols: These focus on reducing the harm from cyber incidents escalated to your full Cyber Incident Mitigation Protocols.

The proper execution of the detect, analyze, and escalate elements during Continuous Vigilance is vital to the success of your Cyber Incident Mitigation Protocols. Those elements combine to ensure that you properly identify and escalate exigent incidents that might inflict significant harm. Moreover, having effective Computing Continuity built into your Continuous Vigilance is equally important because of the heightened ransomware threat.

Organizations need a multidisciplinary team to properly mitigate the harm from exigent cyber incidents.

After you escalate an incident to your Cyber Incident Mitigation Protocols, your multidisciplinary team should deploy the following Cyber Incident Mitigation elements:

Set Team and Initial Plan: This identifies the team members responsible for each escalated incident, who then create an initial investigation plan based on the detection and analysis evidence. Teams need to be set in real-time, because each incident is different, and some personnel might not be available.

Investigate: This focuses on executing your initial investigation plan, which should help you obtain the information needed to contain, eradicate, and/or restore operations. Sometimes, you will proceed directly to the contain, eradicate, and restore phase.

Contain, Eradicate, and Restore: These are grouped because some or all these elements might be needed after the Initial Investigation. Contain means stopping the damage/harm. Eradicate means removing any malicious code and/or unauthorized access or any other source of harm. And restore means restoring operations mostly using your computing continuity plan.

Loop between Investigate and Contain, Eradicate & Restore: This is part of the diagram because when the initial attempts to contain, eradicate & restore are inadequate, a second investigative plan should be created and implemented.

Post-Incident Mitigation: This focuses on reducing any post-incident harm such as by regulatory notifications, privacy notifications, and public relations issues.

Assess and Improve: This focuses on improving your overall cyber risk mitigation efforts by incorporating lessons learned from each instance of detection, analysis, escalation, remediation, and cyber incident mitigation.

When properly and promptly executed, your Cyber Incident Mitigation Protocols can literally stop the loss of millions of dollars, making it essential for cost-effective cyber risk mitigation.

INTEGRATING YOUR INSURANCE COVERAGE, BREACH COACHES, & INVESTIGATION FIRMS:

Ideally, your protocols will integrate your insurance coverage and a set of breach coaches and investigation firms that have been vetted and prepared to help. Practical Cyber includes that service when helping organizations upgrade to Cyber Incident Mitigation Protocols.

ANNUAL TESTING & UPDATING:

As a highly recommended optional service, Practical Cyber provides annual simulations that test a organization's ability to execute its Cyber Incident Mitigation Protocols. This testing includes Practical Cyber reviewing and updating the organization's protocols.

PRACTICAL CYBER AS YOUR 365 INCIDENT MITIGATION ADVISOR:

Companies can engage Practical Cyber to act as their 365 Incident Mitigation Advisor. If an organization confronts a significant cyber-incident -- such as a ransomware attack -- Practical Cyber can it make the best possible decisions, including overseeing outside experts such as a forensic investigation firm and breach coach. While Practical Cyber has extensive incident response experience, it does not offer incident response investigative services or official breach coaching to the organizations. Rather, as part of defense-in-depth, Practical Cyber offers this 365 Incident Mitigation Advisor service that is particularly useful for organizations without full-time CISOs.

DETECTION, ANALYSIS, & MONITORING SYSTEM: As an optional service, Practical Cyber provides organizations a customized cyber threat detection, analysis, & monitoring system that exceeds the results of most Security Information and Event Management platforms (SIEMs). Our Customized Detection, Analysis, & Monitoring System (1) identifies and classifies vulnerabilities before they are exploited and inflict harm; (2) minimizes false positives; and (3) cost-effectively escalates only material incidents to your Cyber Incident Mitigation Protocols. Our customized systems typically cost much less than what an organization would pay for a SIEM such as Rapid7.

ADDITIONAL BENEFITS OF UPGRADING TO OUR CUSTOMIZED CYBER INCIDENT MITIGATION PROTOCOLS

HELPS BUILD YOUR MULTIDISCIPLINARY TEAM: The right multidisciplinary team is essential for cost-effectively mitigating a company's cyber risks. The process of upgrading to Cyber Incident Mitigation Protocols helps organizations create the type of multidisciplinary team needed to cost-effectively mitigate their cyber risks.

FACILIATES THE MULTI-TOOL MITIGATION: Organizations should leverage all five cyber risk mitigation tools. By working with Practical Cyber to adopt customized Cyber Incident Mitigation Protocols – particularly ones that integrate insurance – organizations start developing the skills and experience to more effectively use a multi-tool approach.

SHARPENS YOUR DETECTION, ANALYSIS, & REMEDIATION: Detection, analysis, and remediation are critical aspects of Continuous Vigilance – the core of protecting your company from cyber-attack. During the process of adopting customized Cyber Incident Mitigation Protocols, organizations necessarily sharpen all three areas (detection, analysis, and remediation) by having to evaluate and test each one.

IMPROVES YOUR INSURANCE CYBER RISK TRANSFER: Many organizations are not yet efficiently using insurance to transfer their cyber risks. During the process of adopting customized Cyber Incident Mitigation Protocols, organizations must fully evaluate and understand how their insurance covers cyber-attacks. This process improves their ability to use their insurance to transfer their cyber risks.

CREATES AN EXCELLENT ONGOING RESOURCE: The process of helping a company upgrade to customized Cyber Incident Mitigation Protocols allows Practical Cyber to gain important insights about the company that empowers Practical Cyber to cost-effectively help the company in many ways in the future. This is particularly value for organizations that have not hired full-time CISOs or developed the type of multidisciplinary team needed for success. Moreover, because organizations struggle to retain high-quality cybersecurity personnel, having Practical Cyber fully prepared to help is a major advantage.

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.

Our website explains our services.

BEYOND CYBERSECURITY

Cybersecurity is just one of five tools Practical Cyber uses to help organizations mitigate their client's cyber risks. The five mitigation tools comprise the following:

Appendix B provides more details about our innovative approach.

APPENDIX A: COMMON DEFICIENCIES IN TRADITIONAL INCIDENT RESPONSE PLANS

INSUFFICIENT C-LEVEL SUPPORT & PARTICIPATION: One of the most important aspects of effectively mitigating cyber incidents is to ensure that a representative of leadership is enthusiastically supporting a multidisciplinary approach to cyber incident mitigation and has agreed to participate as the ultimate decision-maker. Leadership matters.

DEFICIENT RESPONSE TEAM COMPOSITION, ROLE DEFINITION, & COMMUNICATIONS: Your cyber incident mitigation team should be customized to your organization and each incident being mitigated. Typically, the team should include outside experts (e.g., a forensic investigation firm), leadership, board of trustees, IT, legal, operations, HR, & potentially PR/marketing. Each member's role must be clearly defined and practiced before incidents occur. And you will need an effective communication system to mitigate incidents.

DEFICIENT INTEGRATION OF INSURANCE AND OUTSIDE EXPERTS: Many organizations have cyber liability insurance but fail to properly integrate it into their incident mitigation. The solution is for an expert – like Practical Cyber – to integrate your coverage into your mitigation efforts, including helping you pick and engage ahead of time the right breach coaches and forensic investigation firms.

LUMPING CYBER INTO COMPREHENSIVE BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN: The people, information, and skills needed for cyber incident mitigation differs materially from those required for other types of challenges such as a natural disaster or pandemic. Therefore, lumping cyber into a larger business continuity and disaster recovery plan obfuscates and degrades your cyber incident mitigation efforts.

DEFICIENT INTEGRATION OF DETECT AND ANALYSIS & INADEQUATE ESCALATION PROCESS: Many traditional incident response plans assume that detection and analysis are being done properly. That is often a mistake because detection and analysis are the essential foundation upon which effective cyber incident mitigation is built. Also, traditional plans often fail to create a clear, customized escalation process with an efficient taxonomy that allows your team to properly analyze and differentiate the potential harm from different incidents.

FAILURE TO TEST PROPLERLY: Many traditional incident response plans are written and forgotten until a cyber incident occurs. Sometimes one or two people will review the plan annually. Both approaches are deficient. Your organization must regularly practice how it will mitigate cyber incidents because (1) the skills and knowledge needed to succeed are esoteric and (2) your organization's ability to react quickly can save millions.

DEFICIENT ASSESSMENT & IMPROVEMENT SYSTEM: Most traditional incident response plans do not have a clear, easy-to-follow process for identifying lessons learned and integrating them into your overall cyber risk mitigation system. In contrast, our Cyber Risk Mitigation Protocols include this type of assessment and improvement system.

APPENDIX B: INTRO TO PRACTICAL CYBER'S MULTI-TOOL, MULTDISCIPLINARY CYBER RISK MITIGATION

WHAT IS OUR INNOVATION?

Multi-tool, multidisciplinary cyber risk mitigation is an innovation that increases profitability by helping organizations (a) invest in only the cyber risk mitigation needed to reduce business-threatening cyber risks to an acceptable level and (b) close sales by proving to clients and partners that you and your offerings are cybersecure.

TWO MAJOR ADVANTAGES

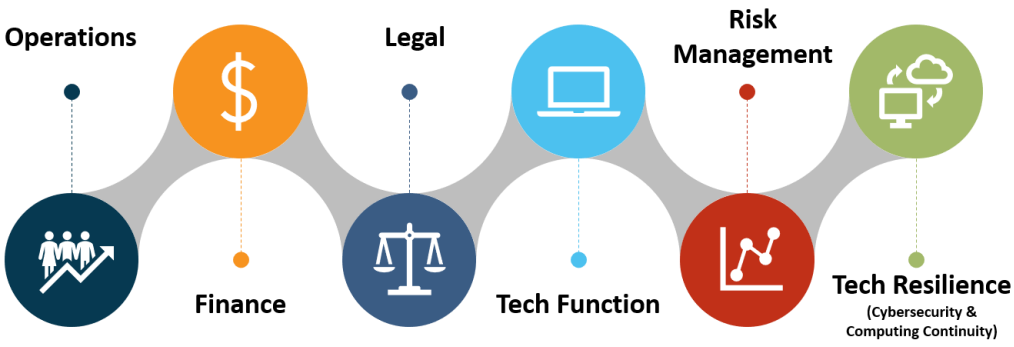
Traditional cybersecurity uses tech, people, and processes to mitigate cyber-attacks. Only recently did it begin using a risk-based approach. Going further, our approach fully leverages (among many other advantages) a Multidisciplinary Approach and the 5 Cyber Risk Mitigation Tools described below.

ADVANTAGE 1: The 5 Cyber Risk Mitigation Tools

Cybersecurity is just one of 5 tools to mitigate your cyber risks & leverage your cyber opportunities.

The graphic to the left shows all 5 Cyber Risk Mitigation Tools, and highlights the need for an auditing and adjustment system for all your efforts.

ADVANTAGE 2: Multidisciplinary Approach



This graphic shows that our approach involves applying the right types of expertise.

Applying this expertise is vital to effectively mitigating your cyber risks and showing your cybersecurity to the world.

DOWNLOAD A DETAILED SUMMARY OF THIS INNOVATIVE APPROACH