PRACTICAL CYBER'S INCIDENT MITIGATION PROTOCOLS

COMMON DEFICIENCIES IN TRADITIONAL INCIDENT RESPONSE PLANS

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 – typically part of a larger business continuity plan.

Unfortunately, traditional cyber incident response plans suffer from a slew of preventable deficiencies explained below.

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 schools 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 school'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.

LEARN MORE ABOUT HOW WE HELP ORGANIZATIONS PREPARE TO MITIGATE ATTACKS THEY CAN'T PREVENT

WHO IS PRACTICAL CYBER?

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.

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