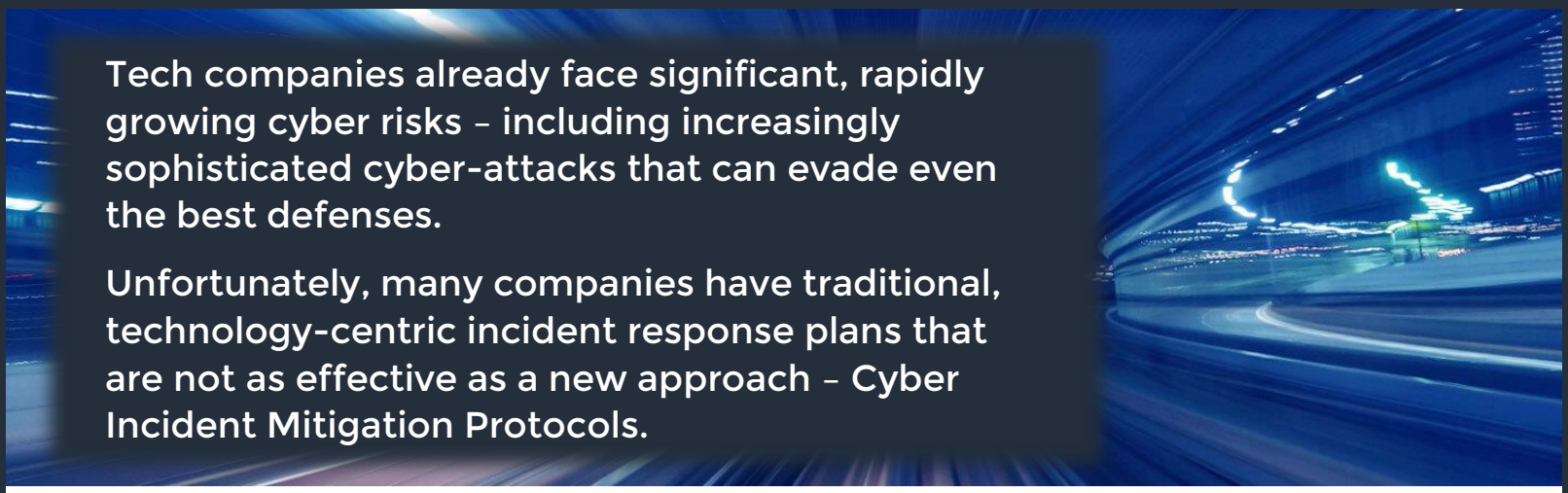
A BETTER APPROACH TO MITIGATING THE HARM FROM CYBER-ATTACKS THAT EVADE YOUR CYBER DEFENSES

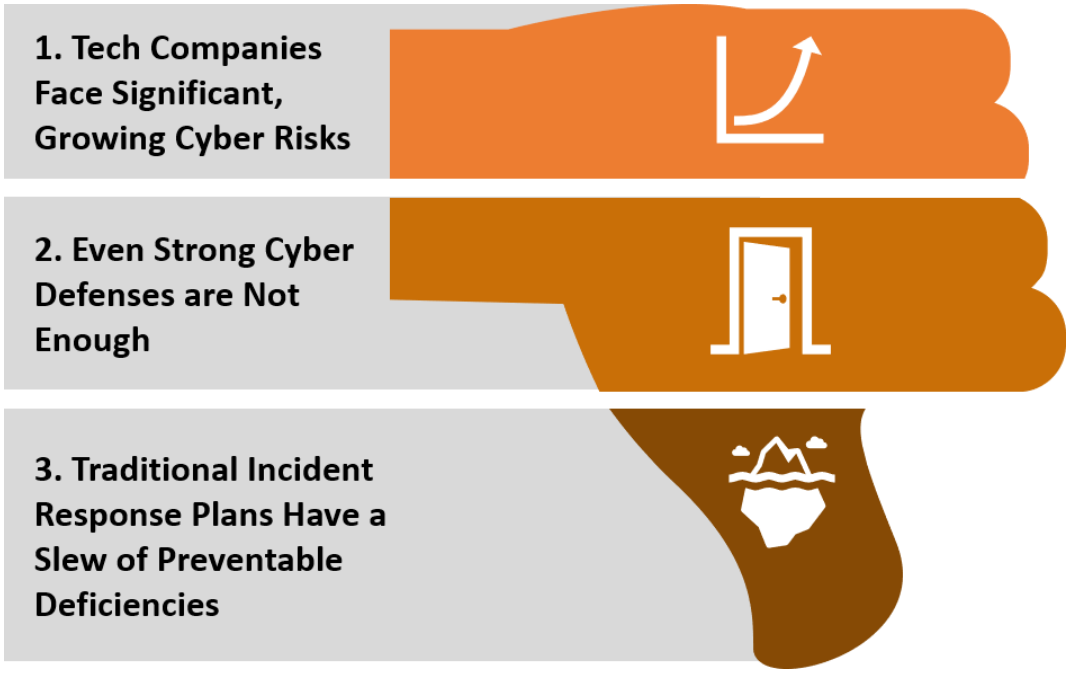


Tech companies already face significant, rapidly growing cyber risks – including increasingly sophisticated cyber-attacks that can evade even the best defenses.

Unfortunately, many companies have traditional, technology-centric incident response plans that are not as effective as a new approach – Cyber Incident Mitigation Protocols.

COMPANIES SHOULD WORRY ABOUT & RE-EVALUATE THEIR TRADITIONAL INCIDENT RESPONSE PLANS

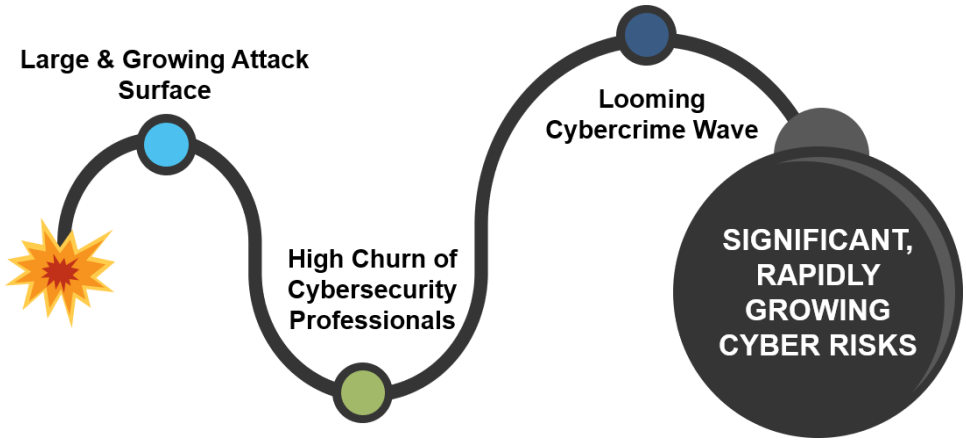
To mitigate the harm from cyber-attacks that evade their defenses, many tech companies have traditional, technology-centric incident response plans. These three factors should make tech companies worry about and re-evaluate their plans:



After explaining these three factors, this article introduces an approach that is more effective than traditional, technology-centric incident response plans – namely, Cyber Incident Mitigation Protocols, which are built upon Profit-Centric, Multi-tool, Multidisciplinary Cyber Risk Mitigation.

1. YOUR SIGNIFCANT, RAPIDLY GROWING CYBER RISKS

This infographic introduces the three main elements creating your significant, rapidly growing cyber risks:



By their nature, tech companies strive to innovate and reduce costs by continuously adding more computing technologies, particularly in these areas:

1. Increased computing power/internet access and new software applications and hardware to deliver their innovative offerings.

2. Sophisticated data analytic technologies (e.g., machine learning and AI) needed to disrupt markets and overcome incumbents.

Each addition of computing technology heightens a company's cyber-attack risks by increasing its cyber-attack surface: i.e., the sum of physical and digital vulnerabilities that can be exploited to carry out a cyber-attack against you. Unfortunately, the attack surface for today's tech companies is enormous and growing at a dangerous time.

High Cybersecurity Professional Churn: The average tenure of Chief Information Security Officers (CISO) in all industries is 26 months, according to the Nominet CISO Stress Report. This churn is a serious problem, both creating high talent search fees and leaving the companies less protected compared with reliable, long-term cybersecurity leadership.

Major, Looming Cybercrime Wave: The economic incentives for cyber criminals are the highest in history, are growing, and are about to generate an unprecedented wave of extortion-based cybercrime, often referred to as ransomware. Most tech leaders understand ransomware basics – namely, that upon infection, it uses encryption to incapacitate computers followed by a payment demand for the means to restore operations. But few leaders know that the recent trend of paying ransoms has created a vibrant ransomware ecosystem that even includes the sale of ransomware software-as-service platforms that come with free trials and tech support. Combined with the rapid increase in the use of computing technologies around the world, this vibrant ecosystem is about to generate an unprecedented wave of extortion-based cybercrimes

exactly when academic institutions have scant money for security/prevention and keep losing cybersecurity personnel at the highest rate ever.

Significant, Rapidly Growing Cyber Risks: Your significant, rapidly growing cyber risks fall into three main categories --

1. Operational interruptions (typically ransomware) – 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. The school also incurred significant investigation costs and untold harm from reputational damage. A reputable cybersecurity company, Sophos, reported that 51 percent of all the businesses it surveyed were hit by ransomware in 2020 and that the average cost was $732,520 without paying the ransom and $1,448,458 with it. These costs, however, do not accurately represent the long-term damage from reputational harm that can be business-threatening to tech companies.

2. Data breaches – Examples include the 218 million accounts stolen from Zynga in 2019, the 538 million accounts stolen from Sina Weibo (the Chinese Twitter) in 2020, the 162 million user accounts stolen from Dubsmash in 2018, and the 150 million user accounts stolen from My Fitness Pal in 2018. Even one of the ultimate tech companies – with unlimited security resources – Microsoft – suffered a data breach of 250 million customer records in 2019. Data breaches cost companies millions. The Ponemon Institute's well-respected report stated that the average United States data breach in 2020 cost $8.64 million. Additionally, smaller breaches like the 1.12 million records stolen from Washington State University in 2019 inflict business-killing damage. Washington State had to pay $4.7 million to settle a class action brought by the data breach victims; and in 2015, the primary teaching hospital for the UCLA school of medicine settled its data breach lawsuit for $7.5 million.

3. IP & financial theft – Tech companies are prime targets for intellectual property theft. This includes the IP theft by foreign government-sponsored attackers – particularly the Chinese – that U.S Intelligence Director warned about in December 2020. He said that the "intelligence is clear: Beijing intends to dominate the U.S. and the rest of the planet economically, militarily and technologically." He described China's approach of economic espionage as "rob, replicate and replace", saying that "China robs U.S. companies of their intellectual property, replicates the technology and then replaces the U.S. firms in the global marketplace." Moreover, this IP theft is the primary goal of Hafnium, the cyber-attack group in China responsible for the Microsoft Exchange Server hacks – as stated above.

These cyber risks represent one of the largest financial threats to universities and colleges. Unfortunately, many companies are using a traditional, technology-centric approach to cyber risk mitigation that is more expensive and less effective than the commonsense multi-tool, multidisciplinary approach; and some are falling prey to the CISO Deficiency.

2. EVEN STRONG CYBER DEFENSES ARE NOT ENOUGH

Cyber-attacks are becoming increasingly sophisticated such as the recent Solarwinds attack and the Microsoft Exchange Server hacks. In early 2020 attackers hacked Solarwinds' software development environment and installed a sophisticated cyber-attack tool (called a backdoor) in the update to Solarwinds' widely used IT monitoring software. By updating their Solarwinds software, customers unwittingly installed a backdoor that allowed the attackers to install additional malware and launch more attacks. Because the overall Solarwinds attack was so sophisticated, it went undetected for months; compromised the computing systems of at least 18,000 Solarwinds customers, including Fortune 500 companies, many US government agencies, and some universities and colleges; and no one knows the extent of the damage.

In early January 2021, cybersecurity experts learned that cybercriminals were actively exploiting 4 newly discovered vulnerabilities (i.e., zero-day attacks) in multiple versions of Microsoft Exchange Server – email and calendaring software widely used around the world. These vulnerabilities helped the attackers steal information and install additional attack tools that facilitate long-term access to the victim's computing networks. According to Microsoft VP Tom Burt, the main cybercriminal group exploiting the vulnerabilities – known as Hafnium – is a "highly skilled and sophisticated" "state-sponsored" group operating from China that "primarily targets entities in the United States" to steal "information from a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks and NGOs." While Microsoft on March 2, 2021 released "security updates" to address these vulnerabilities, the attackers had a long time to use the vulnerabilities to steal valuable information and install covert attack tools. Moreover, according to RiskIQ, 82,731 instances of this software remained insecure (i.e., not updated) as of March 11, 2021.

The Solarwinds attack and the Microsoft Exchange Server hacks emphasize that even tech companies with the best defenses are vulnerable to today's increasingly sophisticated cyber-attacks. This heightened risk increases the value and importance of a company's ability to react quickly and effectively to cyber-attacks that evade its defenses. This in turn places a premium on the effectiveness of your incident response plan.

3. DEFICIENCIES IN TRADITIONAL RESPONSE PLANS

The Underlying Problem – Limits of the Traditional, Technology-Centric Approach to Cybersecurity: The widely used traditional "cybersecurity" approach focuses predominantly on using technologies, people, and processes to protect an organization's computing operations and digital data. Unfortunately, it can involve risky deference by leadership to technologists who while well-intended do not have all the multidisciplinary expertise needed to properly protect companies from their significant, growing cyber risks explained above. This deference can lead to, promote, or exacerbate what we call the CISO Deficiency, which can leave companies unnecessarily vulnerable to cyber-attacks and limits the contributions from the school's non-technologists such as Board of Trustees, in-house counsel, financial professionals, and risk managers. The solution is for companies to adopt Profit-Centric, Multi-tool, Multidisciplinary Cyber Risk Mitigation – which includes the Cyber Risk Mitigation Protocols that replace traditional incident response plans.

The Many Preventable Deficiencies of Traditional Incident Response Plans:

One problem with the traditional cybersecurity approach is the technology-centric incident response plan that many companies have adopted. Traditional incident response plans suffer from a series of preventable deficiencies that leave companies under-prepared to mitigate the harm from unprevented cyber-attacks:

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 companies 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.

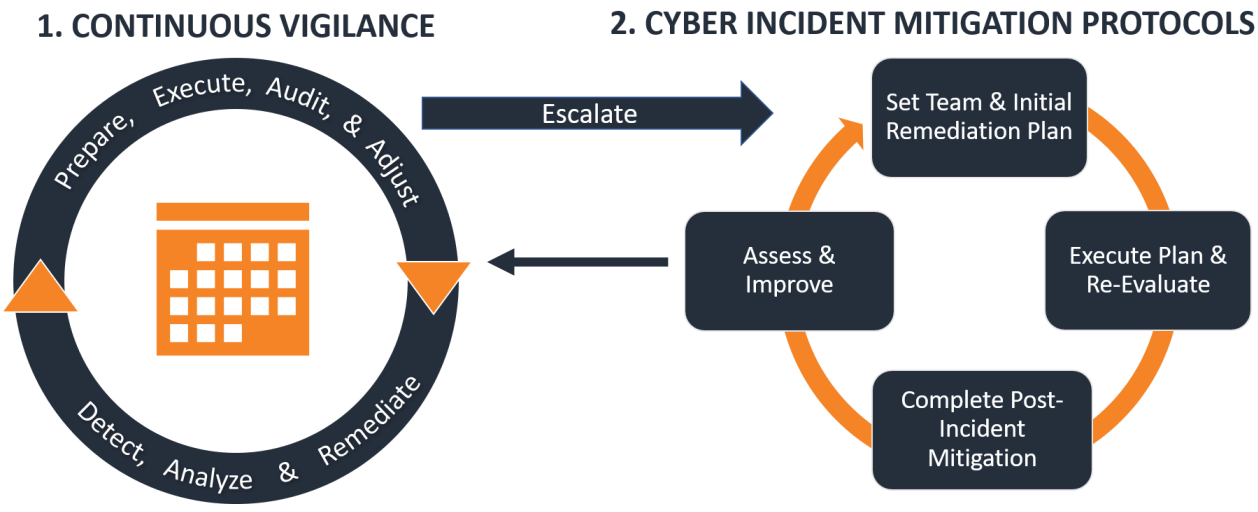
DEFICIENT INTEGRATION OF DETECT AND ANALYSIS & INADEQUATE ESCALATION PROCESS: Many traditional incident response plans assume that detection and analysis are being done properly. That is often a mistake because detection and analysis are the essential foundation upon which effective cyber incident mitigation 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.

THE BETTER APPROACH – CYBER INCIDENT MITIGATION PROTOCOLS

Built Upon Multi-Tool, Multidisciplinary Cyber Risk Mitigation: Practical Cyber used its experience and its innovative Multi-Tool, Multidisciplinary Cyber Risk Mitigation approach to upgrade the traditional incident response plan to more effective Cyber Incident Mitigation Protocols. To upgrade a traditional incident response plan, companies need to understand where their new Cyber Incident Mitigation Protocols fit into an effective, two-part overall cyber risk mitigation system – as this infographic introduces:



The Role of Continuous Vigilance: Continuous Vigilance focuses on everything companies 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 system.

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 (2) to accurately identify and classify cyber 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 cyber risk mitigation tools.

Escalate: This is the process for escalating material cyber incidents to your full Cyber Incident Mitigation Protocols.

The Role of Cyber Incident Mitigation Protocols & How They Work:

Cyber Incident Mitigation Protocols focus on reducing the harm from exigent cyber incidents that Continuous Vigilance does not prevent. The proper execution of the Detect, Analyze, and Escalate elements during Continuous Vigilance is vital to the efficacy of your Cyber Incident Mitigation Protocols. Those elements combine to ensure that you properly identify and analyze all potentially harmful cyber incidents and then only escalate sufficiently exigent incidents to your more costly and time-consuming full mitigation protocols.

After you escalate an exigent cyber incident to your Cyber Incident Mitigation Protocols, your school's multidisciplinary cyber risk mitigation team should deploy the following elements:

1. Set Mitigation Team and Initial Remediation Plan: Cyber Incident Mitigation Teams need to be set for each cyber incident, because each incident is different, and some personnel might not be available. Your Cyber Incident Mitigation Team will use the Detect and Analyze evidence to create an Initial Remediation Plan that can include any mix of these remediation techniques:

Investigate: This involves investigating the cyber incident to determine what if any further action should be taken.

Eradicate: Eradicate means removing any malicious code and/or unauthorized access or any other source of harm.

Contain: Contain means stopping the damage/harm.

Restore: Restore means restoring operations mostly using your Computing Continuity plan

Liability reduction: This covers multiple ways to reduce liability relating to the cyber incident (e.g., insurance notification/approvals, litigation prevention, regulatory compliance, contractual compliance).

Public relations action: This covers any public relations actions need to mitigate the negative impact of cyber incidents.

2. Execute Plan & Re-Evaluate: This focuses on executing the Initial Remediation Plan and evaluating its efficacy. In some situations, evaluating the Initial Remediation Plan reveals the need for further remediation. In these situations, the Mitigation Team must either create new Remediation Plans or modify the Initial Remediation Plan. The Mitigation Team should only end

this part of the process when fully satisfied it has completed all exigent mitigation efforts, and therefore can move on to the next, less exigent phase of "Complete Post-Incident Mitigation."

3. Complete Post-Incident Mitigation: This focuses on completing whatever non-exigent actions are needed to reduce any post-incident harm such as by continuous public relations issues, litigation, and regulatory actions.

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

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

THE BENEFITS OF PRACTICAL CYBER HELPING YOU ADOPT CYBER INCIDENT MITIGATION PROTOCOLS

The main benefit a school receives from Practical Cyber helping it adopt Cyber Incident Mitigation Protocols is enhancing the school's ability to mitigate the potentially devasting harm from unprevented cyber-attacks. This main benefit is facilitated by all the following supporting benefits.

Highly Cost-Effective Stress Test: One of the most common cybersecurity deficiencies is failing to test the efficacy of cyber defenses. Comprehensive testing by an external expert can be cost-prohibitive. However, Practical Cyber's evaluation of your Detect, Analyze, and Escalate systems when helping you create Cyber Incident Mitigation Protocols is a very cost-effective "stress test" of some of the most vital aspects of your cyber defenses. This "stress test" gives companies an excellent, expert-driven, and objective view of the efficacy of main parts of its cyber defenses.

Helps Build Your Multidisciplinary Team: The right multidisciplinary team is essential for cost-effectively mitigating a school's cyber risks. The process Practical Cyber uses to help companies adopt Cyber Incident Mitigation Protocols helps companies develop the type of multidisciplinary team needed to cost-effectively mitigate all their cyber risks.

Facilitates Multi-Tool Mitigation: Companies 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 – companies improve their ability to use all five cyber risk mitigation tools.

Sharpens Your Detection, Analysis, & Escalation: As explained earlier, detection, analysis, and escalation are vital parts of Continuous Vigilance and essential to the efficacy of your Cyber Incident Mitigation Protocols. The process of adopting customized Cyber Incident Mitigation Protocols helps companies sharpen all three areas by having to evaluate and test each one. This improves the efficacy of both your (1) Cyber Incident Mitigation Protocols and (2) overall vulnerability identification and remediation – a major cyber risk mitigation win.

Improves Your Insurance Cyber Risk Transfer: Many companies are not yet efficiently using insurance to transfer their cyber risks. During the process of adopting customized Cyber Incident Mitigation Protocols, companies must fully evaluate and understand how their insurance covers cyber-attacks. This process improves their ability to use their insurance to transfer cyber risks.

Creates an Excellent Ongoing Resource: The process of helping a school upgrade to customized Cyber Incident Mitigation Protocols allows Practical Cyber to gain important insights about the school that empowers Practical Cyber to cost-effectively help the school in many ways in the future. Moreover, because organizations struggle to retain high-quality cybersecurity personnel, having Practical Cyber fully prepared to help is a major advantage.

AN INTRODUCTION TO PRACTICAL CYBER

We are a multidisciplinary cyber and privacy risk mitigation firm driven by the cost-effective integration of these three proven, top-flight experts:

Cybersecurity & Computing Continuity Expert – Dr. Marc Rogers.

Internationally known cybersecurity expert and founder of MKR Forensics.

Tenured Cybersecurity Professor and the Assistant Dean for Cybersecurity Initiatives 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 (e.g., Alissa Gilbert) and alumni with excellent practical experience.

Cyber & Privacy Law + Cyber Risk Transfer 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.

Cybersecurity Researcher, Practitioner, & Pragmatist – Alissa Gilbert Ph.D. Candidate.

Nationally ranked ethical hacker. Highly skilled vulnerability tester.

One of the top cybersecurity researchers in the United States. Many years of practical experience protecting organizations from cyber-attack

COO of CircleCityCon, an elite cybersecurity conference.

Ph.D. candidate and instructor at Purdue University.