PRACTICAL CYBER
Pragmatic + Elite = Greater Protection

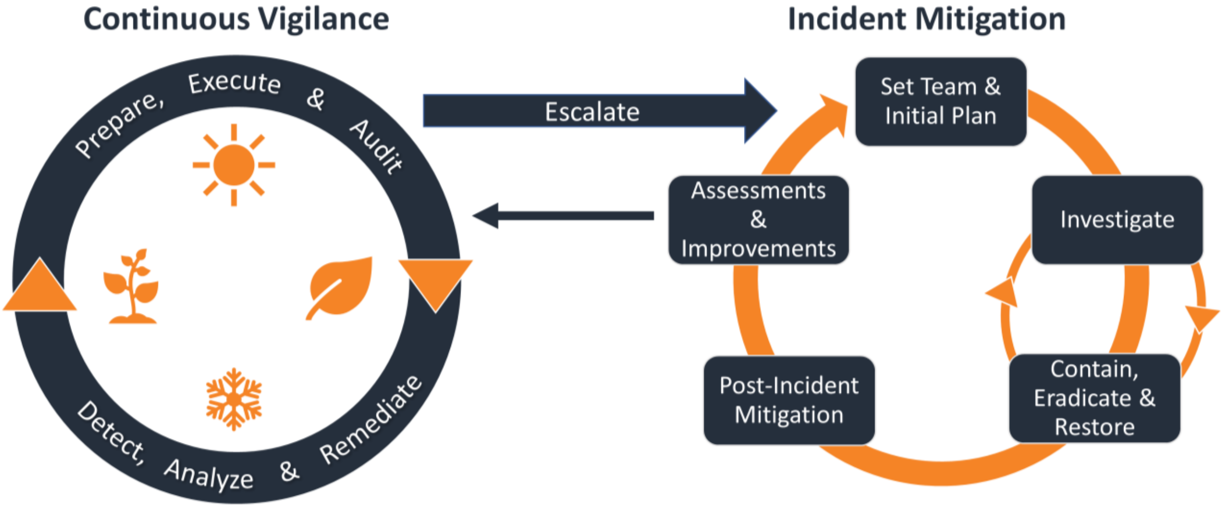
HOW OUR CYBER RISK MITIGATION SYSTEMS WORK

June 2019

FAR BEYOND THE TRADITIONAL APPROACH

The traditional approach to mitigating cyber risk is to adopt some form of cybersecurity – e.g. firewalls, anti-virus software, employee policies, etc. – a cyber incident response plan, and haphazardly try to transfer some cyber risk via contract and insurance.

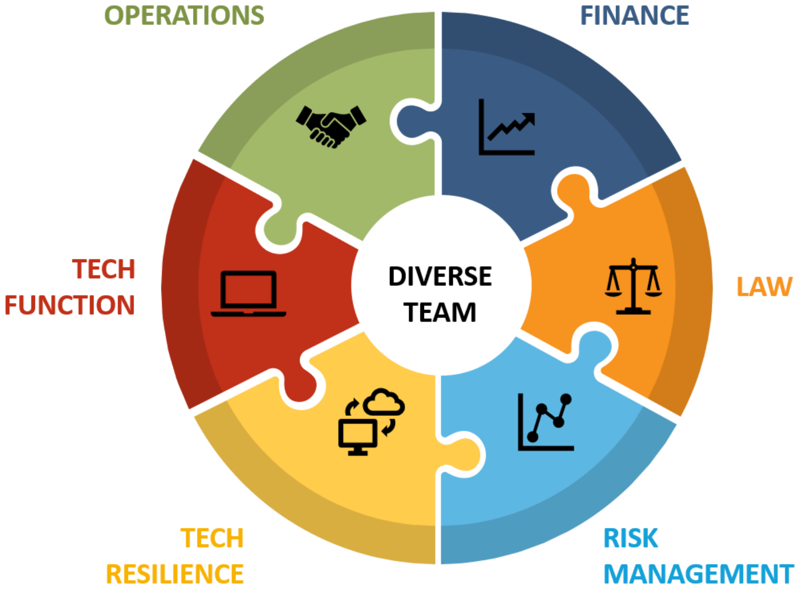
Our Cyber Risk Mitigation Systems materially exceed the efficacy of this traditional approach. As this graphic introduces, these systems have two parts:



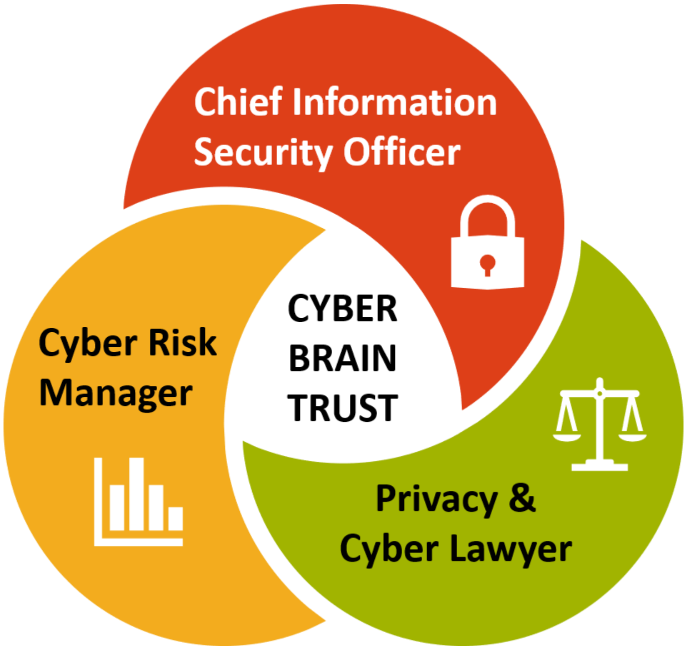
Continuous Vigilance focuses on everything you should do to mitigate cyber risks before an exigent cyber requires immediate remediation.

Incident Mitigation focuses on reducing the all the harm (particularly financial) from any cyber incidents escalated to your Incident Mitigation protocols.

To create these systems, we deploy a multidisciplinary team – operations, finance, legal, risk management, technology resilience, and technology function:



We incorporate your internal resources, and we supply the Technology Resilience (both cybersecurity and business continuity), Legal (privacy and cyber law), and Cyber Risk Management expertise via our Cyber Brain Trust:



Cybersecurity Expert – Purdue University’s Dr. Marc Rogers

Internationally known cybersecurity expert.

Executive Director Purdue Cyber Security and Forensics Lab and graduate program (the number one program in the nation).

25+ years practical cybersecurity experience enhanced by academic career.

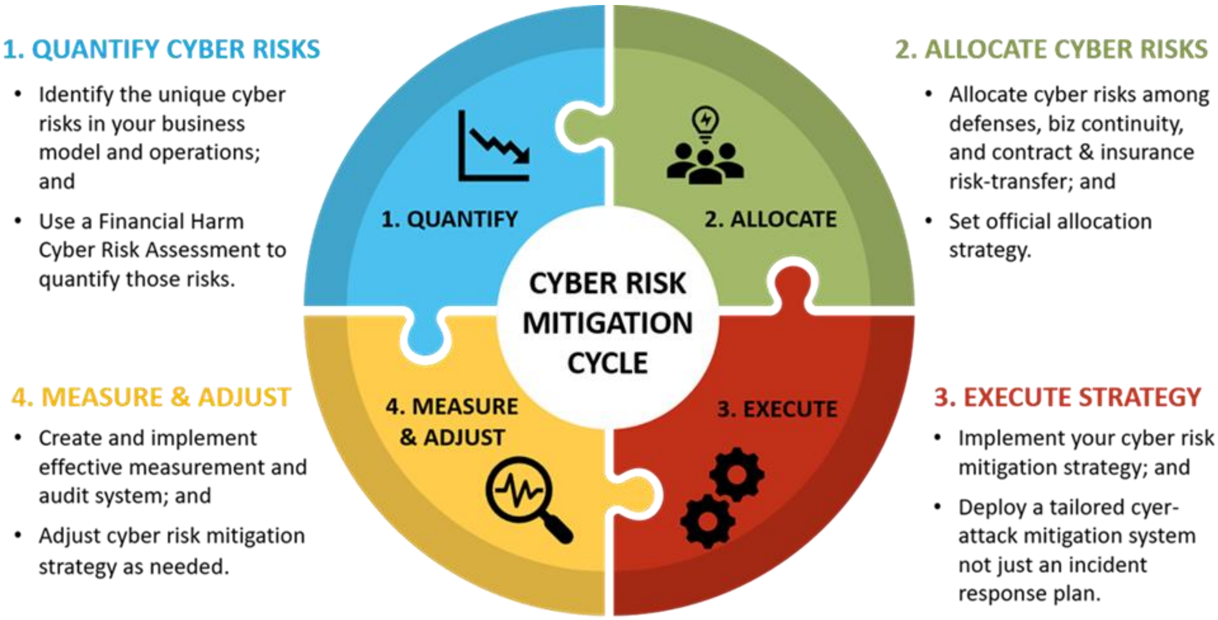
Privacy & Cyber Lawyer + Cyber Risk Expert – Elliot Turrini

Former federal cybercrime prosecutor and cyberlaw/privacy attorney in private practice.

Cyber risk mitigation expert, including ERM and cyber liability insurance.

Editor & Author of Cybercrimes: A Multidisciplinary Analysis.

The collective multidisciplinary team applies this Cyber Risk Mitigation Cycle:



1. QUANTIFY CYBER RISKS

- Identify the unique cyber risks in your business model and operations; and
- Use a Financial Harm Cyber Risk Assessment to quantify those risks.

2. ALLOCATE CYBER RISKS

- Allocate cyber risks among defenses, biz continuity, and contract & insurance risk-transfer; and
- Set official allocation strategy.

4. MEASURE & ADJUST

- Create and implement effective measurement and audit system; and
- Adjust cyber risk mitigation strategy as needed.

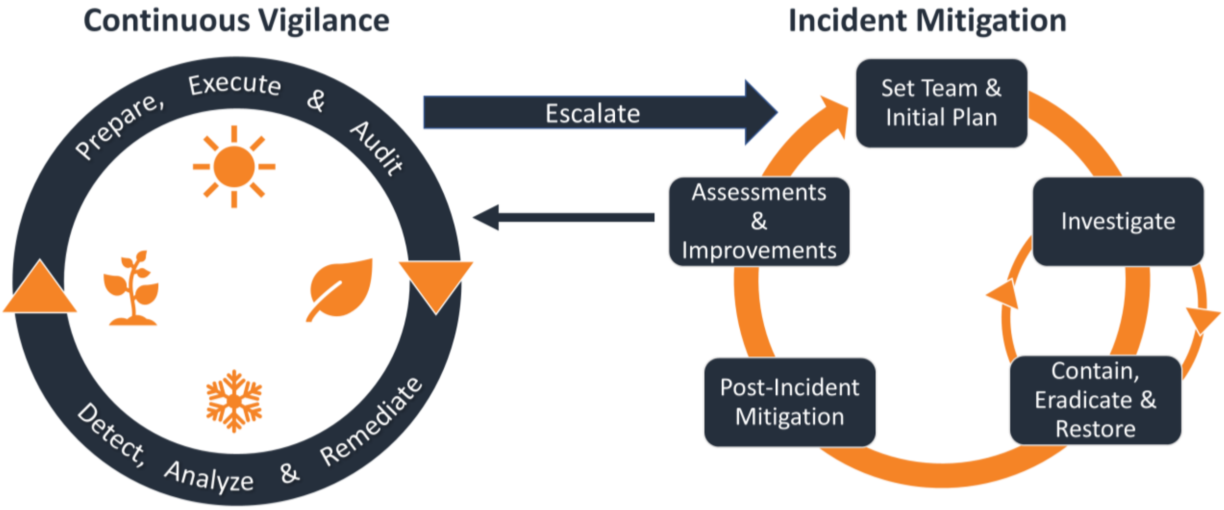
3. EXECUTE STRATEGY

- Implement your cyber risk mitigation strategy; and
- Deploy a tailored cyer-attack mitigation system not just an incident response plan.

The end result is an effective Cyber Risk Mitigation System customized to your unique business model, operations, and risks.

DETAILS OF CYBER RISK MITIGATION SYSTEMS

This section details how we help you create your customized Cyber Risk Mitigation System.



CONTINUOUS VIGILANCE

Continuous Vigilance focuses on everything your company should do to mitigate its cyber risks before it identifies an exigent cyber incident that needs immediate, extensive remediation.

It involves a 24/7, 365 day/year dynamic integration of these elements:

Prepare: Involves the first two parts of the Cyber Risk Mitigation Cycle -- setting your overall cyber risk mitigation strategy by (1) identifying and quantifying your unique cyber risks and (2) allocating those risks among defenses, business continuity, and contract and insurance risk-transfer. It also includes setting up and staffing the Incident Mitigation part of your CRMS – e.g. training employees to adeptly handle cyber incidents, picking the right experts (e.g. breach coach, cyber investigation firm, and PR consultant) and incident mitigation team alternates ahead of time, and preparing your full cyber incident mitigation team via mock cyber incidents.

Execute: This involves implementing your cyber risk mitigation strategy – e.g. strong defenses, effective business continuity, and the right risk-transfer via contract and insurance.

Audit: Involves creating and implementing an effective measurement and auditing system for your CRMS.

Detect & Analyze: Involves 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 Incident Mitigation Protocols.

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

Continuous Vigilance is complex and constitutes the core of your cyber risk mitigation.

Each element described above plays a vital role. Your organization will benefit greatly from continuing to use its multidisciplinary team to diligently integrate and apply all the elements. The main benefit is materially reducing your cyber risks by preventing potentially devastating cyber incidents from ever happening.

Here, prevention can literally mean the difference between profits and bankruptcy. But, 100% prevention is impossible, which means that your organization should also invest in a customized Incident Mitigation System.

INCIDENT MITIGATION

Incident Mitigation focuses on reducing the harm (particularly financial) from any cyber incidents escalated to your Incident Mitigation Protocols. Your Incident Mitigation System is set-up during Continuous Vigilance, which should be done by your multidisciplinary team.

The proper and dynamically execution of the Detect, Analyze, and Escalate elements of Continuous Vigilance is vital to the success of your Incident Mitigation System. Those elements collaborate to ensure that you properly identify and escalate the material cyber incidents that can inflict significant financial harm.

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

Set Team and Initial Plan – This identifies the team members responsible for each escalated cyber 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'll proceed directly to the contain, eradicate and restore phase.

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

Loop between Investigate and Contain, Eradicate & Restore – This is part of the diagram because when the initial attempts to contain, eradicate & restore don't succeed fully, 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 System by incorporating lessons learned from each instance of Detection, Analysis, Escalation, and Incident Mitigation.

When considering the benefits of a strong Incident Mitigation system, don't fixate on data breaches. Remember that today's cyber-attacks are fast, effective, and can shut down your operations via attacks like NotPetya.

When properly and promptly executed, your Incident Mitigation System can literally stop the loss of millions of dollars. It is essential to your cost-effective mitigation of cyber risks.

MORE INFORMATION

For more information try our website or contact Elliot Turrini at (201) 572-4957 or Elliot@PracticalCyber.com