PRACTICAL CYBER – Pragmatic + Cutting-Edge = Greater Protection

INCIDENT RESPONSE & MITIGATION PLANS

INNOVATIVE APPROACH TO CYBER INCIDENT RESPONSE PLANS THAT COST-EFFECTIVELY MITIGATE HARM

INTRODUCTION TO CYBER INCIDENT RESPONSE AND MITIGATION

"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

John Chambers, Executive Chairman and former CEO Cisco Systems

Cyber incidents continue to become more prevalent, sophisticated and faster. Businesses continue to become more heavily dependent on computers and digital information systems. Computing technologies and the Internet continue to get faster.

Together, these realities decrease the time that organizations have to react to cyber incidents, increase the potential financial harm, and make it even more important to diligently prepare for cyber incidents. In some situations, being unprepared can mean the end of your organization's existence.

A "cyber incident" is any event that threatens the security, confidentiality, integrity, or availability of your electronic information assets, information systems, and/or the networks that deliver the information. Examples include:

- Unauthorized entry, scans, or probes
- Modification or destruction of data
- Denial of service
- Ransomware attacks, malicious code or viruses
- Networking system failure (widespread)
- Application or database failure (widespread)

A cyber incident response and mitigation plan prepares an organization to react quickly and effectively to minimize financial losses from cyber incidents and any related interference with their mission. The best plans are customized to your organization's mission and operations, kept current, and practiced regularly.

OVERVIEW OF PRACTICAL CYBER'S CYBER INCIDENT RESPONSE AND MITIGATION PLANS

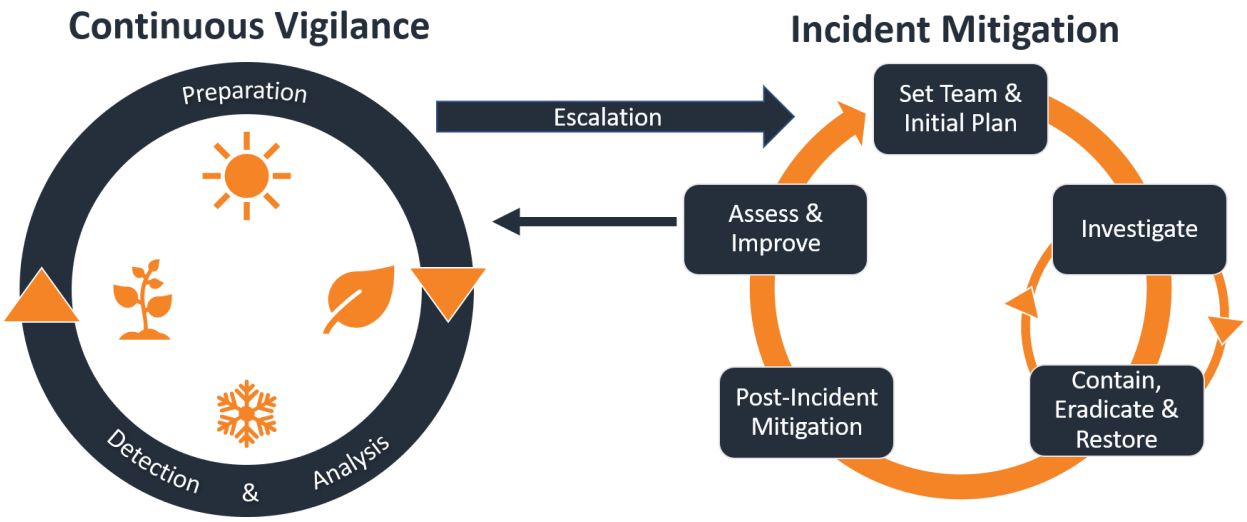
MINIMIZE HARM FROM CYBER INCIDENTS

We tailor your Cyber Incident Response & Mitigation Plan (CIRMP) to your unique situation – people, business operations, computing systems, and insurance – so it will help you efficiently minimize harm from cyber incidents. Examples of harm from cyber incidents include:

- Destruction or modification of your computing technologies and/or electronic information
- Revenue loss from interruptions to your operations and/or injury to your reputation
- Legal and regulatory liability
- Theft of your digital information
- Contractual penalties from customers
- Excessive incident response costs – e.g. legal fees, IT investigation costs, and PR costs

WRITTEN EFFICIENT AND TAILORED PLANS

Based on interviews and a review of your IT systems and business operations, Practical Cyber provides you a customized CIRMP that sets forth efficient procedures for the following:



Continuous Vigilance: It focuses on ensuring you are always prepare to react quickly and effectively to all types of cyber incidents:

- **Preparation –** This includes having strong customized cyber defenses, training employees to adeptly handle cyber incidents, picking the right experts (e.g. breach coach, cyber investigation

firm, and PR consultant) and incident response team alternates ahead of time, and preparing your full cyber incident response team via mock cyber incidents.

- **Detection and analysis –** These focuse on promptly and efficiently identifying, analyzing, and classifying cyber incidents to minimize false positives and cost-effectively escalate only material incidents to the Incident Mitigation protocols

- **Escalation –** This is the process used to escalate material cyber incidents to the Incident Mitigation Protocols.

Incident Mitigation: It focuses on mitigating the harm from the cyber incidents that are escalated to the Incident Mitigation protocols. It includes a dynamic approach to these 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.

- **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 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 restore operations typically using your business continuity plan.

- **Loop between Investigate and Contain, Eradicate & Restore** – This is part of the diagram because at time 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 incident response plan by incorporating lessons learned from each instance of Detection, Analysis, Escalation, and Incident Mitigation

Organizations that diligent create and maintain an integrated approach to Continuous Vigilance and Incident Mitigation are taking important steps toward protecting themselves from cyber incidents and attacks.

PRACTICAL CYBER'S CYBER INCIDENT RESPONSE AND MITIGATION EXPERTISE

Practical Cyber uses the combined expertise of Dr. Rogers and Elliot Turrini to provide innovative, customized, and cost-effective cyber incident response and mitigation plans.

Purdue University's Dr. Marc Rogers

Internationally known cybersecurity expert

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

Excellent practical experience while a professor at Purdue:

- Led over 125 cyber incident response investigations – including several for Fortune 100 companies;
- Created over 100 cyber incident response plans – including for several Fortune 50 companies.
- His clients have spanned various industries including technology, financial services, healthcare, manufacturing, etc.

Former Federal Cybercrime Prosecutor Elliot Turrini

Former federal cybercrime prosecutor where he handled the Melissa Virus prosecution; the UBS insider attack case; and other major investigations and prosecutions

Cyberlaw and privacy attorney in private practice – covering all aspects of cyber and privacy law

Editor & Author of Cybercrimes: A Multidisciplinary Analysis – a book published 2010 – covering all aspects of cybersecurity

VP of Consulting Services Arete Advisors, a cybersecurity firm, 2017

General Counsel & EVP of 300 employee IT services firm 2004-07

Enterprise risk management and cyber liability insurance expert

Contact Practical Cyber:

Elliot Turrini – Elliot.Turrini@PracticalCyber.com – (201) 572 4957