PRACTICAL CYBER – Pragmatic + Cutting-Edge = Greater Protection

INNOVATIVE FINANCIAL HARM CYBER RISK ASSESSMENTS

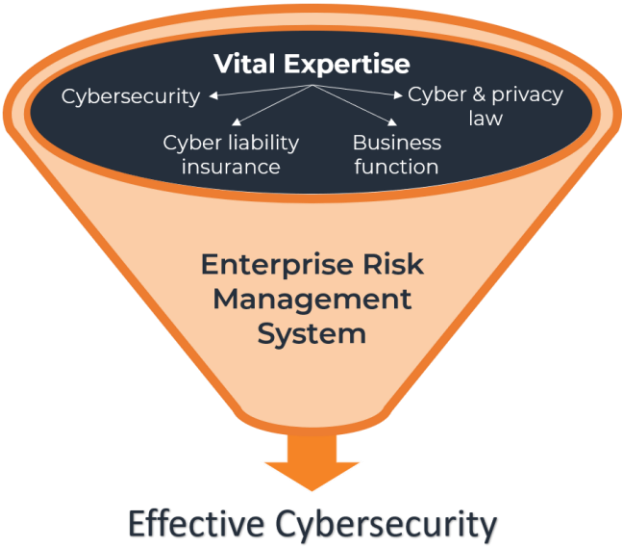
INNOVATIVE APPROACH TO CYBER RISK ASSESSMENT THAT HELPS YOU COST-EFFECTIVELY PREVENT HARM

INTRODUCTION TO FINANCIAL HARM CYBER RISK ASSESSMENTS

The goal of all cybersecurity is to prevent cyber attacks from inflicting financial harm or otherwise impeding an organization's mission. While there's no one-size-fits-all approach, almost every expert agrees that cybersecurity should include a cyber risk assessment.

But, most cyber risk assessments focus predominantly on Interference Risks – i.e., the risks that cyber attacks will "interfere" with the availability, confidentiality, or integrity of your computing technologies (hardware, internal software, and external software) and/or your electronic information. Interference Risk Assessments are important; and doing them properly requires strong cybersecurity expertise. Unfortunately, Interference Risk Assessments divulge too little about your financial risks and how to mitigate them. This leaves you uncertain about how to best allocate your limited resources to protect your business operations and mission from cyber-attack.

In contrast, Practical Cyber's innovative cyber risk assessments – known as Financial Harm Cyber Risk Assessments – quantify your cyber risks by deploying (1) proven Enterprise Risk Management principles and (2) expertise in cybersecurity, privacy & cyber law, business function, and cyber liability insurance.



Financial Harm Cyber Risk Assessments are the best assessment technique for helping organizations make cost-effective decisions about what cyber defenses to adopt, what risks to internalize, and what insurance to buy.

DETAILS ABOUT OUR CUSTOMIZED FINANCIAL HARM CYBER RISK ASSESSMENTS

Our Financial Harm Cyber Risk Assessments are customized to your people, business operations, IT systems, and insurance. They are innovative because to properly identify and quantify your cyber risks, they use proven Enterprise Risk Management principles and scrutinize your cybersecurity, privacy & cyber law, and cyber liability insurance issues.

Here's an overview of our assessment methodology:

- Start by listing the ways that cyber incidents can inflict financial harm on your unique business model, including estimating probability and fiscal impact of different cyber incidents. This might include creating a customized financial model for your organization.
- Conduct an Interference Cyber Risk Assessment, namely, assess the processes, policies, people, and technologies that comprise and protect your electronic information systems and electronic data – looking for vulnerabilities and improvements.
- Predict your potential out-of-pocket costs from cyber incidents by analyzing your insurance coverage. (If you don't have a cyber liability insurance policy, you can conduct a "gap" analysis of your existing insurance; but it is probable that without a dedicated cyber policy, you won't have adequate coverage.)
- Suggest cybersecurity improvements and additional insurance coverage -- including quantifying the value and costs – to help you better mitigate your cyber risks.

Organizations should use the valuable information produced by Financial Harm Cyber Risk Assessments to guide their implementation of a customized, dynamic and continuous cybersecurity strategy that includes (at least) strong technological defenses, employee policies & training, and a cyber incident response and mitigation plan.

The valuable information that your Financial Harm Cyber Risk Assessment produces should be the centerpiece of your cybersecurity strategy and program.

PRACTICAL CYBER'S EXPERTISE BEHIND ITS CUSTOMIZED FINANCIAL HARM CYBER RISK ASSESSMENTS

Our cybersecurity expertise is both pragmatic and cutting-edge because it is delivered through Dr. Marc Rogers. He is the Director of the top academic cybersecurity program in the nation, and possesses outstanding real-world, pragmatic experience. To enhance the value that Dr. Rogers delivers, former federal cybercrime prosecutor Elliot Turrini adds his mix of enterprise risk management, cybersecurity & privacy law, and cyber insurance expertise. Together, they deliver outstanding cybersecurity services.

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