Webinar – The Right Stuff: Validating Reasonable Information Security

Michael A. Gold, co-chair of JMBM's Cybersecurity & Privacy Group, will host a panel of industry leading experts for the webinar, The Right Stuff: Validating Reasonable Information Security.

Date: Thursday, June 18, 2020
Time: 10 AM – 11:15 AM PDT; 1 PM – 1:15 PM EDT

Register Now

Most organizations have never had to prove that they have reasonable information security. Business and legal pressures are changing this dramatically. The California Consumer Privacy Act exposes businesses that have been breached to serious financial liability when they do not have reasonable information security. With data breaches increasing in scope and damage regardless of the money spent on cybersecurity, businesses will need to validate – in effect prove – that they have reasonable information security in order to avoid financial, legal and reputational harm.

During this webinar, our panel of experts cover:

The meaning of reasonable information security: What is it? Why the established information security frameworks, such as NIST, ISO and CISO, do not deliver reasonable information security; Why dynamic assessment of an organization's information security posture is crucial; The impact of overlooked vulnerabilities in cloud and IoT environments.

The legal requirement for validating reasonable information security: The far-reaching impact of the California Consumer Privacy Act's requirement for reasonable information security practices and procedures; Why the law is a precursor to similar requirements likely to be adopted by other states and the federal government; Legal exposures arising from inability to validate reasonable information security.

The business and insurance imperatives for validating reasonable information security: Cyber insurance carriers will no longer take at face value an insured's representations about its information security posture; Larger enterprises will decline to do business with companies that cannot validate the effectiveness of their information security measures; Regulated companies will no longer be permitted to self-certify their compliance with information security and privacy requirements.

Validating reasonable information security: The importance of process; Identifying and measuring material cyber risks across expanded ecosystems; The documentation necessary to validate reasonable information security; The governance structures needed establish, maintain and prove reasonable information security; Selecting the validation team; The report of the validation assessment.

MODERATOR:
Michael A. Gold, Partner, Co-Chair, Cybersecurity and Privacy Group
Michael counsels organizations in a wide range of information security and privacy matters, including legal compliance, breach responses, forensic investigations, and crisis management. He was named one of the “Top 20 Cyber – Artificial Intelligence Lawyers” by the Los Angeles Daily Journal (2018), one of the “Most Influential Lawyers: Digital Media and E-Commerce Law” by the Los Angeles Business Journal, and has been designated a “Top Rated Lawyer in Technology Law” by Martindale Hubbell.

PANELISTS:

Art Ehuan, Vice President, Crypsis
Art has extensive experience as a Chief Information Security Officer (CISO) for a financial services/insurance corporation and interim CISO for a multinational health care management corporation, an international manufacturing company, a multinational oil/gas organization and a government treasury agency.

Heather Wilkinson, Senior Broker, Willis Towers Watson
Heather Wilkinson is a Senior Broker and founding member of Willis Towers Watson’s Cyber team. She currently works as WTW’s national cyber resource as a risk consultant on large, complex risks.

Ed Cabrera, Chief Cybersecurity Officer, Trend Micro
Ed is responsible for analyzing emerging cybersecurity threats to develop innovative and resilient enterprise risk management strategies for Fortune 500 clients. Before joining Trend Micro, Ed was a 20-year veteran of the United States Secret Service where he served as the Secret Service CISO where he was responsible for establishing and maintaining a global information security and data privacy program to protect Secret Service data information assets and systems.

Register Now for this important program. There is no cost to attend.

JMBM’s Cybersecurity and Privacy Group counsels clients in a wide variety of industries, including accounting firms, law firms, business management firms and family offices, in matters ranging from development of cybersecurity strategies, creation of data security and privacy policies, responding to data breaches and regulatory inquiries and investigations, and crisis management. The Cybersecurity and Privacy Group uses a focused intake methodology that permits clients to get a reliable sense of their cybersecurity readiness and to determine optimal, client-specific approaches to cybersecurity.