Phenomenati

Cybersecurity 201
for the Board of Directors

This is a 1-2 hour informational session with your Board of Directors; delivered by senior IT executives, each with decades of experience in IT modernization, digital transformation, IT governance, and information "cyber" security. The session provides a strategic horizon scan of business, technology, threat, risk, and cyber security trends unfolding in the 2020s. The objective is to prepare your Board and Officers for the new Risks emerging this decade.

Technology Evolution

The session begins with a brief introduction of today's dynamic and evolving digital landscape, selecting relevant subjects from a broad set of topics, including…

- Augmented Reality, Virtual Reality, Gamification, and Virtual Assistants
- Social networks, & Influence Brokering
- Cross-channel, multi-media integration
- Market demographics tracking & analytics
- Consumerization of Deep Fakes
- Artificial Intelligence, and specifically Machine Learning
- Internet of Things (IoT)
- Networks from personal pico-nets, to 5G wireless, to nation-state isolation.
- Demystifying "Cloud" Computing
- Hyper-converged infrastructure
- Software Defined Everything
- Zero Trust Architecture
- Blockchain, and
- Quantum Computing

Growing Vulnerability

Next the group will focus on trends in the Vulnerabilities related to these evolving and emergent technologies, including:

- People, Processes, Technologies – Everything has an “Attack Surface”
- Engineering without Analysis & Design – “Agile” Everything trades discipline and diligence in favor of responsiveness and time-to-market
- Increasing dependency on 3rd party component technologies
- Complexity impedes Business Impact Analysis. Complexity obfuscates Dependency. Dependency invites Risk.
- Public obsession with bug bounties over secure development
- Technical Debt and Extreme Business Models (from *complacency* to frenetic *risk-taking*) impede the defender
- Time, Money, and Scale favor the attacker

Compounding Consequences

Finally the session addresses the proverbial “So What?” question, by looking at the potential range of Consequences.

- The loss of ***Control*** from the growth in hidden dependencies.
- The rise of ***Dis-Continuity*** of Operations due to complex, brittle infrastructures lacking Resiliency and Survivability
- The end of personal and professional ***Privacy***.
- The loss of Client ***Trust***, due to lost ***integrity*** of business processes, products, and services.
- The erosion of ***Market Share***, ***Incomes*** and ***Profits*** due to breaches in Confidentiality, Integrity, and Availability.
- The expansion of Corporate (fiduciary) ***Liability*** for poor Due Diligence and Due Care
- The end of provable ***Truth***, and the power of Manipulating Perceptions – politics, economies, market competition, etc.

Unimpeded Threat

Targeting these expanding Vulnerabilities is a wave of continuous adaptation in Threat Actor tactics, techniques, and tools.

The Threat Spectrum spans from mischievous hackers, to Organized Crime, to Nation States, to malicious and unwitting Insiders.

Threat Techniques & Objectives Continuously Evolve:

- Novelty is introduced and becomes Commodity on a daily basis.
- Stolen information (identities, credentials, intellectual property) fuels Fraud, Extortion, and Unfair Competition
- Compromised integrity (Dis-information/Mis-information) is the foundation for powerful, yet subtle manipulation
- Destruction of availability (from DDoS to Ransomware) threatens nations and businesses of all sizes.

Threat has become Big Business:

- Crime in the Shadows – the ever changing “Dark Web”
- Politics in the Shadows – reputation con/destruction for hire
- Global Conflict in the Shadows – Cyber Warfare, Perception Warfare, Cyber Mercenaries

On Wrapping Up...

Phenomenati’s “Cyber Security 201 for the Board” is a concentrated look at the digital landscape, designed to get your Board of Directors and Executive team focused on both current and future trends on the horizon that may have significant positive and negative impact on the organization.

The primary outcome of this session is alignment with respect to the emergent trends, vulnerabilities, threats and potential consequences that are worthy of ongoing monitoring and scrutiny by your leadership team.

www.phenomenati.com | info@phenomenati.com