Phenomenati

Cybersecurity 101 for the Board of Directors

This is a 1-2 hour educational session with your Board of Directors; delivered by experienced executives certified in cyber security, IT/IS auditing, and risk management. It provides a concise and effective way to get your Board and Executive team on the same page with respect to Governing your Risk Mitigation, Cyber Security investments, and regulatory Compliance (e.g., GRC).

Concepts

The session with your Board will begin with clear definitions of a few core concepts – ***Trust***, ***Risk***, and ***Security***.

Every professional relationship is based on Trust. It takes years to build, but only minutes to destroy. And it is based far more on what you Do, than what you Say. Especially before, during, and after a breach.

Risk is an abstract concept, but will be decomposed into its fundamental elements – ***Threats***, ***Vulnerabilities***, and ***Consequences***. How each relates to Cyber Security will be discussed.

As the reciprocal of Risk, Security involves investments in mitigating "***Controls***" that should be prioritized and employed (or not) based on the potential consequences to the business.

The full range of Cyber Security Controls (administrative, physical, and technical) will be introduced at the conceptual level. Further, a straightforward methodology for performing Cost/Benefit analyses will be presented as a possible foundation for strategic decision making.

Due Diligence

The session continues, acknowledging Due Diligence as a core fiduciary responsibility.

Informed Decisions demand due diligence based on comprehensive ***Intelligence***. In Cyber Security, this includes Knowing your ***adversary***, Knowing ***yourself*** (dependencies and vulnerabilities), and being able to anticipate ***Consequences***. The same applies to evaluating the cyber security posture of prospects for potential mergers & acquisition.

Board members will learn how to assess an organization's cyber risk intelligence, and how well that informs decisions (reject, accept, mitigate or transfer) that affect its overall ***Risk Posture***.

It is not possible to be "100% Secure", so investments must be prioritized based upon solid ***business cases***. The Board will learn to develop and apply ***Risk Scenarios*** to capture and summarize ***Risk Assessments*** (qualitative and/or quantitative) that will prioritize and govern all strategic decisions.

Due Care

The third strategic topic to be covered is Due Care. Here the Board is charged with ensuring the organization properly invests in a reasonable level of mitigation for the Risks that have been identified.

For Cyber Security, such Due Care will take the form of a comprehensive ***Cyber Security Strategy*** for the organization. Effective programs typically leverage an industry-recognized "***framework***" as a means to organize, prioritize, and communicate all aspects; including a range of "***Controls***" (administrative, physical, and technical) and the day-to-day "***Operations***" of those controls.

Recognized frameworks will be introduced, and the range of potential controls will be summarized at a non-technical level; including policies, procedures, technologies (e.g., Identity, Authentication, Authorization, Auditing, Access, etc.), and their continuous operation.

Assessments, Audits, and Certification

The fourth and final major topic addresses the core principle of "***Trust, But Verify***".

Most organizations will be required by their stakeholders to ***demonstrate*** a commitment to continuous assessment and continuous improvement.

Such activities can include informal ***self-assessments*** (ideally best based on a recognized framework), public ***compliance*** assertions, formal ***external audits***, and ultimately ***3rd party Certifications*** which summarize and attest to the organization's appropriate levels of Due Diligence and Due Care.

The processes for Assessment, Audit, and Certification will be discussed; and the set of relevant industry standards will be briefly introduced, including ISO 27000, NIST, AICPA SOC 2, HIPAA-HITECH, PCI DSS, GDPR, CCPA, etc.

On Wrapping Up...

All contemporary businesses, but especially Digital Transformation initiatives, confront an unprecedented level of Risk. There will be compromises.

This session will prepare the most senior levels of your organization to oversee and govern your cyber security and risk mitigation programs effectively. Ensuring your levels of Due Diligence and Due Care are optimized for the business and compare favorably to the "Reasonable Person" standard.

www.phenomenati.com | info@phenomenati.com