POLARIS RISK
GLOBAL RISK IS OUR BUSINESS

Polaris Presents:

Board & Leadership Cybersecurity Consulting

Cybersecurity isn't only an IT problem – it's a company-wide responsibility. Ransomware, phishing attacks, and malware are unfortunate facts of modern business. Remote work, cloud solutions, and international conflicts have made cyberattacks frighteningly common – prompting the intervention of the Securities & Exchange Commission ("SEC"). *Under **new SEC regulations**, certain Boards are required to detail their oversight of cyber-risks, while also overseeing swift incident disclosure and robust, proactive risk management*.

However, *Boards and Executives may not have the dedicated time, team, budget, or technical knowledge needed to contend with quick-shifting cyber risks* – especially as attacks continue to scale in pace and scope, and as new threats to IP, customer data, and operations drive concerns among employees and partners. But Polaris' Cybersecurity Board & Leadership Consulting services free leadership to focus on broader strategy, while a dedicated expert(s) accounts for cyber risks.

New Threats, New Expectations

With cyberattacks growing more frequent and more costly, regulators and investors are now demanding unprecedented levels of transparency, expertise, and preparedness.

Changing Compliance Standards

On July 26, 2023, the Securities & Exchange Commission ("SEC") adopted new cybersecurity, governance, and incident disclosure standards. These rules require certain companies to provide annual statements attesting to their cyber-risk management and leadership; companies are now expected to disclose cybersecurity incidents within days, while consistently maintaining proactive risk management efforts. These changes demand more proactive, organized cyber defenses.

Growing Leadership Expectations

New SEC standards also require that Boards disclose their cybersecurity expertise. While Board Members are not required to become cybersecurity experts, knowledge of key cyber threats, solutions, and trends may help assuage potential misgivings from regulators and investors.

Board & vCISO Consulting Services

Attackers are constantly innovating destructive new breach methods, and new, insidious strains of ransomware and malware. These fast-changing threats demand dedicated attention – though many companies don't have the bandwidth to maintain internal cybersecurity teams, experts, or CISOs. Polaris, and its stable of expert advisors and consultants, can offer the focused expertise your security requires.

Board & Leadership Trainings

Polaris offers detailed trainings on clients' inherent cyber-risks and defenses. Trainings contextualize industry-wide risks and emerging threat trends within the strengths, liabilities, and opportunities of a client's unique risk profile. The result is a balanced understanding of both broad risks and client-specific solutions and strategies. Polaris can provide regular security awareness trainings and "tabletop"/simulation exercises on potential cyber incidents to test a company's ability to respond.

Developing Cyber Policies, Procedures, & Strategy

With new threats developing daily, cybersecurity profiles can often feel indefinite. To ensure that leadership can speak to their cyber exposure, compliance, governance, data/privacy protection, and risk management, Polaris' experts can assess, revise, or oversee cyber strategies and procedures.

Expert, Affordable vCISO Consulting

If you're a small to midsize company, you can affordably bring outside cyber expertise in-house with a Virtual Chief Information Security Officer ("vCISO"). This expert collaborates with company leaders and IT teams to devise and execute cybersecurity strategies customized to your threat profile. They will be available to the client's internal team as needed – and will still be afforded full access to Polaris' sophisticated suite of cybersecurity tools, trainings, and techniques.

Leveraging Metrics for Efficient Coverage

Polaris will work with your IT teams to understand and analyze operational cybersecurity data. This data will be used to develop meaningful, board-level metrics. Reports will be provided to the board through an ongoing, sustainable reporting process, ensuring that data remains focused and relevant.

Meet Evolving Rules & Regulations

Assess Your Cyber-Risk Posture

Develop & Deploy Cyber Expertise