POLARIS
CORPORATE RISK MANAGEMENT

Assessing Your Cyber Resilience with Polaris' **Cyber Readiness Assessments**

Though cyberattacks target your digital environment, they pose a real-world threat to your company's operations. Recent breaches, ransomware attacks, and data leaks have targeted providers across finance, education, healthcare, IT, retail, and other major industries.

Each attack represents an evolution in attackers' software and strategy, as bad actors adapt their tools and strategies to innovative technologies. To outmaneuver fast-evolving cyber risks, your company needs safeguards that are as sophisticated as the crimes themselves.

As the rate of cyberattacks increases, companies the world over must assess their cyber readiness. With Polaris' **Cyber Readiness Assessment** – our detailed, easy-to-follow checklist of cybersecurity necessities – we offer clients actionable insights into the strengths and vulnerabilities present in their network and organization.

External & Internal Vulnerability Tests

Your network's strengths and weaknesses are made frighteningly clear in the aftermath of an attack. Breaches offer critical insight into your cybersecurity posture, as they reveal the precise location and nature of your company's vulnerabilities. Thankfully, you do not need to suffer a true attack to evaluate the security of your systems: during External & Internal Vulnerability Tests, Polaris' expert assessors accurately and effectively identify your network's vulnerabilities – resulting in a prioritized list of practical, actionable recommendations.

Social Engineering & Email Defenses

A growing majority of cyber breaches rely on "social engineering" – manipulative tactics used to extract sensitive information from unsuspecting employees and vendors. Through deceptively designed emails, links, and attachments, attackers "bait" team members into downloading malware, revealing critical passwords/protections, or disclosing sensitive data. To prepare companies for this threat, Polaris offers safe and controlled "phishing" simulations. These customized, sophisticated test attacks measure your workforce's threat awareness and response, while also assessing the effectiveness of your email filtering and authentication protocols.

Security Controls, Configuration & Compliance

Given the startling frequency of cyberattacks and ransomware incidents – and their growing reach across industries, markets, and services – attacks on your network infrastructure are not a question of if, but when. A ransomware attack will more than likely target your company; when it does, you will want to be certain that your network's security controls can mitigate the attack's spread. To assess whether your network is equipped to swiftly identify and contain a ransomware attack, Polaris evaluates your technical controls – or the configuration/settings of your network, systems, software, tools, and more. This review offers client's confidence in their security controls, while also assessing compliance with relevant industry standards and regulations.

Response & Recovery Program

When assessing cybersecurity readiness, Polaris' assessors emphasize not only resistance, but resilience – a company's ability to respond to and recover from cyberattacks, consistently and continuously. Should a cyberattack infect your network's infrastructure, your security and stability will depend on decisive, confident responses; only urgent actions will effectively mitigate an attack's spread and scale. Polaris' Response & Recovery Programs help your team navigate the critical stresses and decisions that follow ransomware and other cyberattacks, with guidance on how to efficiently restore services and processes, manage legal repercussions, and direct public relations – while evaluating your information and data backup/restoration processes in real-time.