POLARIS
CORPORATE RISK MANAGEMENT

RAPID INCIDENT RESPONSE

THREAT ANALYSIS & RECOVERY

CYBER RISK READINESS ASSESSMENT

Urgent & Effective Ransomware Incident Response

While ransomware attacks can often feel abstract or limited to the digital world, the Colonial Pipeline attack of May 2021 is a reminder of the real-world threats that cyberattacks can pose to operations and vital infrastructure. This threat extends across a range of industries, as recent targets have included educational institutions, IT services companies, healthcare providers, and retailers. With attacks growing more frequent, the FBI, Homeland Security, and other critical security agencies warn of continued efforts by Russia's SVR, North Korea's Lazarus Group, or more nimble groups in the vein of Babuk or DarkSide to cause havoc.

Can your company afford that risk?

Should an incident occur, Polaris can help you reclaim control of your operations. For a flat fee, Polaris provides reviews of key policies, post-action audits/assessments, forensic analyses, malware removal and more following an incident.

POLICY REVIEWS & ASSESSMENTS

Given the frequency of ransomware incidents – with as many as 200 million attacks occurring annually – organizations often prioritize ransomware response before ransomware preparedness. Polaris, however, offers a more holistic approach, helping you to draft and enact policies – including standards for data backups, employee trainings, and anti-viral software – that mitigate exposure risks. Whether augmenting plans or composing new strategies, Polaris can tailor procedures to your company's specific risk posture.

RAPID RESPONSE

As soon as just one employee falls for a phishing scam – clicking on a seemingly innocuous link, in a seemingly legitimate email – the countdown begins; within one minute of a breach, malware can spread through your entire organization, grinding your operations to a halt. How, then, can your company recover? Polaris can provide the guidance and services you need to fight back – all with the speed that cyber risks demand. Call Polaris, and within only six hours help will be on the way.

MALWARE REMOVAL

Once infected, your devices, networks, and systems will need to be cleaned of any infesting malware or ransomware; even after an initial incident, malicious files and software programs can lie dormant in your company's systems for days, weeks, months, or years. To help regain control of a client's IT infrastructure, Polaris offers surgical, thorough cyber-attack agent removal services, as our experts ensure that malware, ransomware, and other cyber threats are cleansed from your devices and utilities.

POST-ACTION AUDITS & ASSESSMENTS

Incidents can destabilize your company and cause weeks of downtime, highlighting your vulnerabilities and revealing elements of your risk posture that need strengthening. To ensure that your company addresses these vulnerabilities, Polaris can review your teams' readiness for further cyber-attacks, while closely monitoring your cyber infrastructure in case the issue re-emerges. A detailed analysis and post-action assessment from Polaris can lead to refined, refocused policies, trainings, and responses.

DIGITAL FORENSIC COLLECTION & ANALYSIS

In the aftermath of an incident, it is essential that your company preserves and analyzes the digital "fingerprints" left by an attacker. Polaris, through its detailed digital forensic reviews and analyses of breached servers, server logs, devices, and relevant accounts, can identify any discernable anomalies in the wake of a cyber-attack. This process may illuminate the methods or identities of the perpetrators – details which can be parlayed into a more comprehensive investigation.

ONLINE INVESTIGATION & ANALYSIS

Following a forensic inquiry, Polaris can launch a prompt, pointed investigation through online sources that can mitigate your losses or liability while safeguarding your activity and reputation. Whereas forensic analyses might retrieve digital evidence, our investigators leverage and expand that evidence using a specialized suite of investigative tools to probe the Deep/Dark Web, and more. These searches may offer insight into bad actors involved in the scheme, or their rationales.