MANDIANT

DATASHEET

CYBER INSURANCE RISK ASSESSMENT

A high-level risk assessment for insurance underwriting

BENEFITS

- Identification, classification and analysis of cyber risk
- Identification of factors that could cause an organization to experience a financial loss
- Identification of company and industry cyber threats
- Strategic recommendations for improvement
- Provide insurance underwriters the information needed to evaluate the risk level of the insured

Why Mandiant

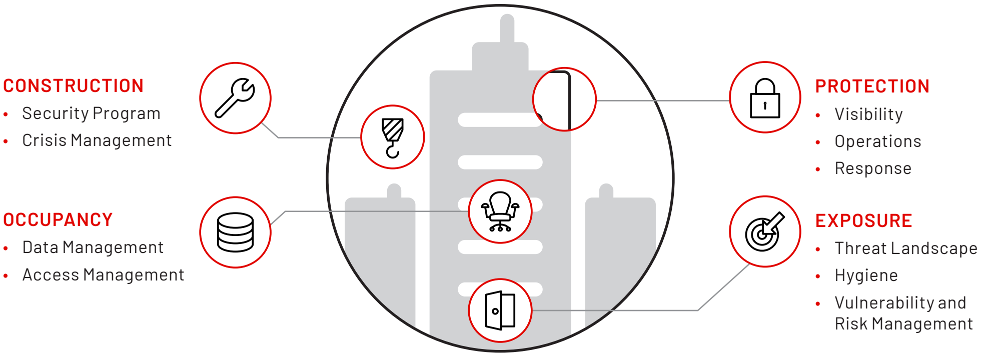
Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Service Overview

The Cyber Insurance Risk Assessment draws on Mandiant's knowledge of advanced threat actors, experience responding to security breaches, and extensive expertise evaluating security programs maturity and readiness. It is specifically designed to provide a quick, high-level evaluation of an organization's risk level based on their technology, processes and people to facilitate the identification, classification and analysis of cyber risk for insurance underwriting. Risk is assessed along the four elements of the property insurance underwriting framework known as C.O.P.E.: construction, occupancy, protection and exposure. C.O.P.E. has been extended to apply to the assessment of technology-driven risk.

Methodology

This two-week engagement combines a general risk level assessment based on the organization's industry, size and geography with cyber risk scoring across the four C.O.P.E. domains. By overlaying the general risk assessment across the four security domains and multiple subdomains, a weighted risk score is derived to determine the risk posture for each domain and the company as a whole.



CONSTRUCTION
- Security Program
- Crisis Management

OCCUPANCY
- Data Management
- Access Management

PROTECTION
- Visibility
- Operations
- Response

EXPOSURE
- Threat Landscape
- Hygiene
- Vulnerability and Risk Management

FIGURE 1. C.O.P.E. based cyber risk insurance domain.

DELIVERABLES

- Cyber Insurance Risk Assessment Report
  - Executive Summary
  - Identification of current capabilities and risk levels by domain
  - Strategic recommendations for improvement
- Executive presentation
- Threat Assessment Report

TABLE 1. Domain Descriptions.

Construction	Occupancy	Protection	Exposure
Evaluate how the information security program is structured, identifying strengths and areas with opportunity for improvement. Areas reviewed include: • General information technology policies and procedures • Policies and procedures for incident response, including breach notification and crisis management • Staffing • Senior management and leadership awareness • Audit and compliance practices	Review data and asset management processes, including: • Classification policies • Technical controls to manage data • Encryption usage requirements • Data retention policies • Backup and recovery policies • Standard asset build and control requirements for items such as laptops, serves and mobile devices	Review how well the organization is protected by technology, processes and people deployed for detection, analysis, response and containment of advanced cyber attacks. This includes threat visibility, operational security capabilities and incident response capabilities.	Determine risk exposure by assessing the threat landscape for the industry, type of business and geographic regions where the organizations operates. • Review effectiveness of established processes and policies for identifying business and information security risk • Review system and network maintenance policies to determine adequacy of existing controls • Review processes and policies for vulnerability assessment and remediation, logging requirements, log management, end point, cloud and mobile protection and logging, internal and external penetration testing and remediation of identified vulnerabilities

Learn more at **www.mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT