



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.



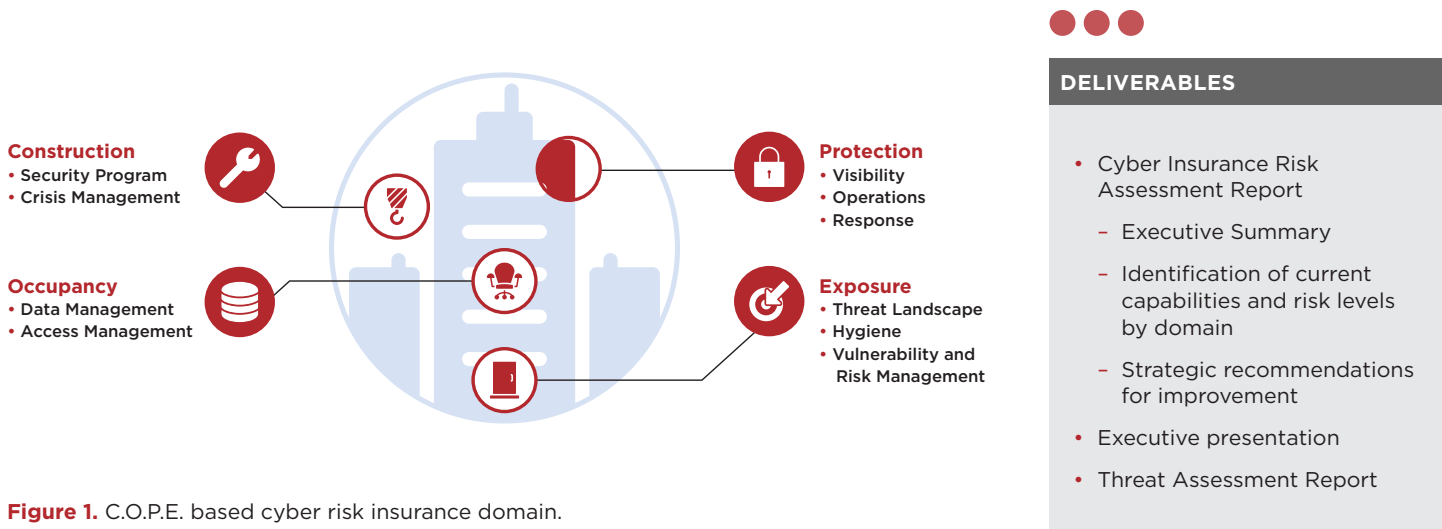


Figure 1. C.O.P.E. based cyber risk insurance domain.

Domain Descriptions

Construction	Occupancy	Protection	Exposure
<p>Evaluate how the information security program is structured, identifying strengths and areas with opportunity for improvement. Areas reviewed include:</p> <ul style="list-style-type: none"> • 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 	<p>Review data and asset management processes, including:</p> <ul style="list-style-type: none"> • 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, servers and mobile devices 	<p>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.</p>	<p>Determine risk exposure by assessing the threat landscape for the industry, type of business and geographic regions where the organizations operates.</p> <ul style="list-style-type: none"> • 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

For more information on Mandiant consulting services, visit: www.FireEye.com/services.html

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
 408.321.6300/877.FIREEYE (347.3393)
 info@FireEye.com

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. DS.CIRA.US-EN-072018

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

