COALFIRE℠

Cyber Risk Program Maturity Assessment

UNDERSTAND AND MANAGE YOUR ORGANIZATION'S CYBER RISK.

In today's escalating cyber risk environment, you need to make sure you're focused on the right priorities by first understanding the threats facing your organization and the assets that must be protected. Let Coalfire give you valuable insight that will help you optimize your risk management activities.

WHAT IS YOUR COMPANY’S CYBER RISK EXPOSURE?

While this question seems relatively simple, the answer isn’t as straightforward. Compliance doesn’t equal security, and threats seem to evolve on a daily basis. As a result, your answer is likely a resounding “maybe.” And you’re not alone. According to a 2015 NYSE Governance Survey, 66% of public company board members are not fully confident their companies are properly protected against a cyber attack.

As cybersecurity advisors, Coalfire can help you identify and understand threats and vulnerabilities so you can manage cyber risk the same way you manage other risks – proactively, comprehensively, and effectively. Coalfire’s Cyber Risk Program Maturity Assessment is a high-level evaluation of key elements of your organization’s risk management program. Our experts assess your security posture, compare your environment to similar organizations, and provide a prioritized roadmap. From the assessment, you’ll be able to:

- Understand how you are managing cyber risks, including third-party risk.
- Take your risk management activities to a more effective level.
- Ensure efficient development and/or optimization of your cyber program.
- Maximize your return on investment in cybersecurity.

THE DIMENSIONS OF A CYBER RISK PROGRAM

Coalfire will assess your cyber risk program by evaluating your capabilities across multiple dimensions.

Risk management

Methods, frameworks, policies, and processes used to assess and treat cyber risk

- Does your security team understand your industry's current threat landscape?
- How frequently are risk assessments performed?
- Has your security team identified your organization's most valuable assets?
- Who participates in the process and when?

Governance, compliance, and assurance

Policies and procedures that ensure risk-related decisions are made according to company policy and with appropriate oversight

- Are the board and senior management routinely updated on cyber risk management efforts?
- Are metrics used to monitor progress toward stated goals?
- Do you receive audit reports and/or independent assessments of control effectiveness?

Security organization

The human resources, both in-house and via third parties, deployed to define, operate, and manage security controls

- Can the security organization structure appropriately meet objectives?
- Does the organization have adequate skills and capacity to perform its duties?

Security technology

Technical controls and solutions used to identify, detect, protect, respond, and recover from cyber threats

- Has your team deployed an appropriate set of security technologies and controls?
- Are security solutions functioning as intended, and are they adequately supported?

Third-party risk

Tools, policies, and procedures to ensure that vendors, service providers, and partners manage risk associated with their data, systems, and processes

- Do contracts with third parties have terms and conditions that address cybersecurity requirements?
- Does your security team test and/or audit third-party security?

Threat and vulnerability management

The people, processes, and technology that anticipate, detect, and respond to threats that could impact data, systems, and networks

- Can you analyze threat data and quickly respond?
- Are you receiving industry-specific threat insights and vulnerabilities?
- Does your organization have adequate reporting and escalation procedures?

Incident management

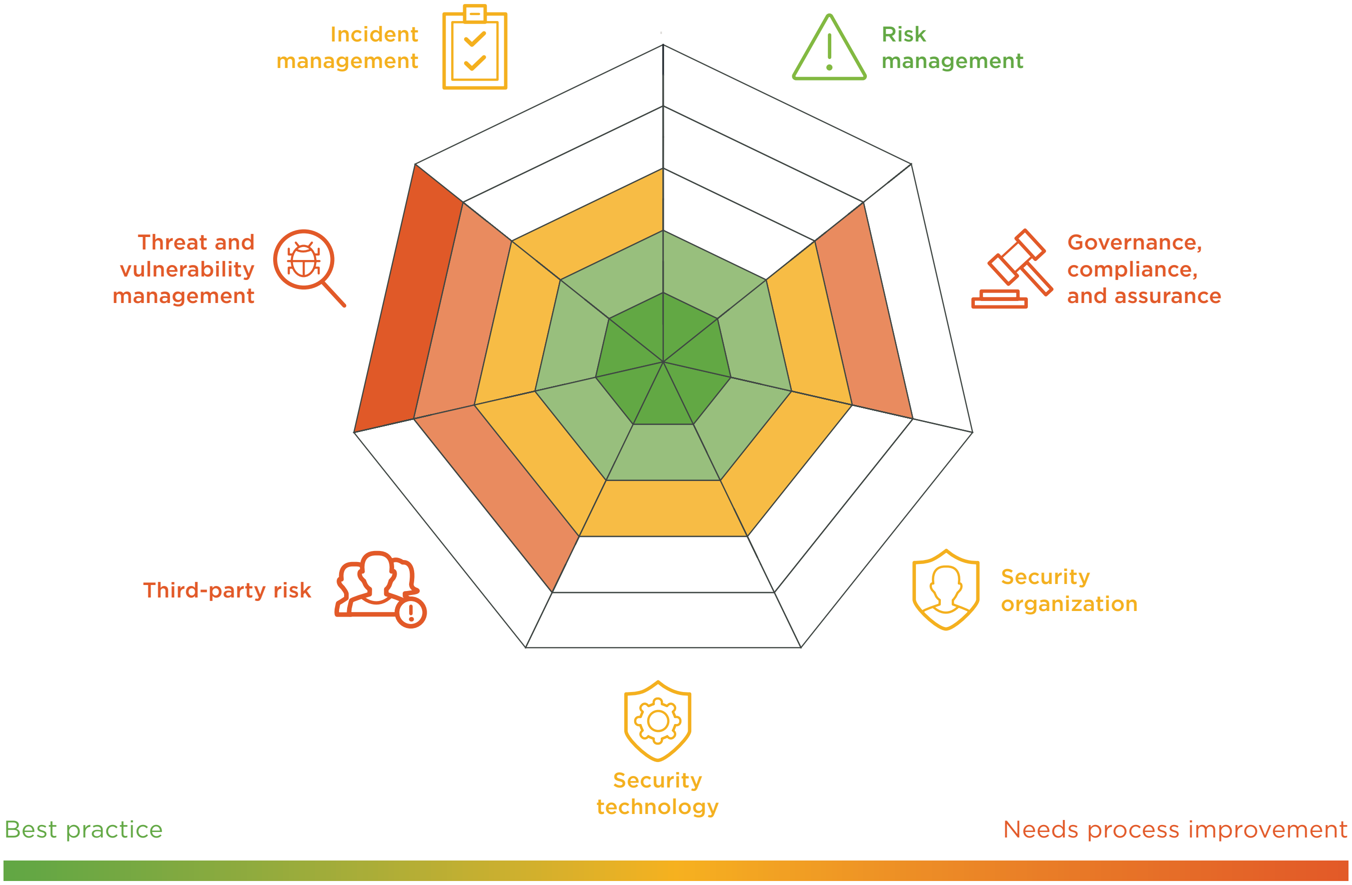
The resources and procedures for detecting, responding, and recovering from cyber incidents

- Is your incident response plan (IRP) consistent with your organization's structure and policies?
- Do you receive after-action reports on incidents and completed exercises?

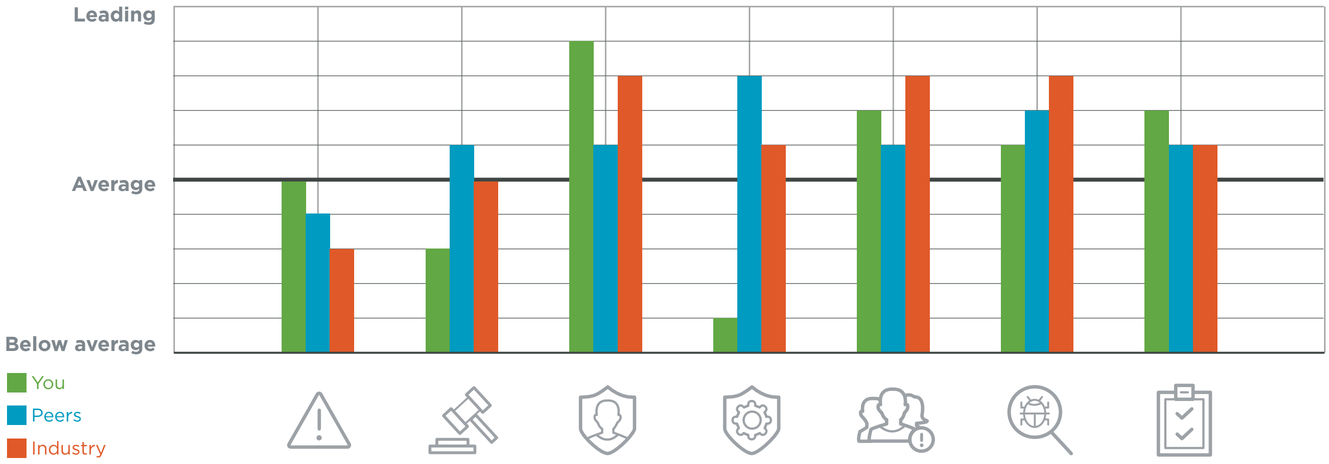
DELIVERABLES

You will receive a maturity assessment and a comparison of your capabilities in relation to your peers.

Maturity rating



Peer comparison



YOUR ROADMAP TO EFFICIENT, EFFECTIVE CYBER RISK MANAGEMENT

Designed specifically as a solution for directors and senior management, our maturity assessment provides valuable insight into the effectiveness of your cyber risk program. We explore your current security posture, and then compare it to cross-industry best practices and your peers. From there, we provide:

- A written summary report that rates your organization's maturity across each dimension of our program assessment model relative to peer organizations
- Actionable recommendations that can improve your program maturity to targeted levels
- An onsite presentation to management, where we explain our findings and recommendations and answer questions related to the assessment

What is a cyber risk program?

The collection of measures (people, processes, and technology) taken by an enterprise to anticipate and control for risks related to the use of data, computers, and networks.

LEARN MORE ABOUT COALFIRE'S CYBER RISK MATURITY ASSESSMENT.

coalfire.com | 877-224-8077

The nation's cyber risk management and compliance leader

A leading provider of IT advisory services, Coalfire has more than 15 years in IT security and compliance. We empower organizations to comply with global financial, government, industry, and healthcare mandates while helping our clients build the IT infrastructure and security systems that will protect their businesses from security breaches and data theft. Our approach leverages the CoalfireOne Platform of software services and tools, which is purpose-built to support customer compliance and risk management. In fact, they're the very same tools our auditors rely on.