COALFIRE

DATASHEET

# Enterprise cyber risk assessment

Defining your enterprise cyber risk posture

Businesses are adopting new economic models for managing their technology infrastructures, taking advantage of scale, architecture, third-party providers, and the automation these technologies provide. While these initiatives are designed to improve cost models and enterprise extensibility, they present new cyber risk considerations.

- 10.9% of organizations' IT budgets are spent on cybersecurity.
- Organizations with better security hygiene experience nearly a one-third reduction in breaches.
- According to Gartner, in 2020, 100% of large enterprises will be asked to report to their boards on cyber risk.

## BUSINESS VALUE DRIVERS

| Executive | Operational | Regulatory |
|---|---|---|
| • Improved decision-making criteria | • Enhanced risk management | • Compliance assurance |
| • Strategic planning enablement | • Prioritization of risk-reduction activities | |
| • Heightened risk awareness | • Identification of new risks and threats | |

## TYPICAL CHALLENGES TO UNDERSTANDING ENTERPRISE RISK

Due to advancing technologies and cloud services, many organizations have highly disparate and extended system boundaries and endpoints. This paradigm shift makes it difficult to understand how data, services, and infrastructure are secured in an environment managed and maintained across multiple platforms.

Compliance attestations (e.g., SOC, PCI Attestation of Compliance [AOC]) are good places to start, but they don't communicate the full picture of enterprise risk associated with these new technologies and services. Shared resources, administrative access, data governance, privacy, and configuration management present challenges in managing security across various platforms.

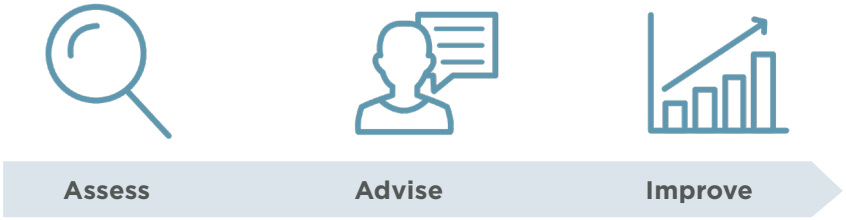
**Common questions that must be addressed include:**

- What additional cyber risks does your organization face when deploying services across multiple platforms?
- Aren't security and risk managed by your service provider(s)?
- What is your liability exposure should the data with your third-party service provider get compromised?
- How do you balance the benefits of your service providers' platforms while protecting your company's sensitive data?

## ADVANTAGES OF PERFORMING AN ENTERPRISE RISK ASSESSMENT

As more organizations increase reliance on third-party service providers and plan more migrations to cloud service providers, senior and business leadership must understand the risks and security impacts of extending sensitive data and business support services beyond their traditional controls.

Enterprise cyber risk assessments help you identify shortcomings in managing the new operational environment, while providing leadership with visibility into the cyber risks present in your organization. As your organization becomes more informed of your cyber risks, you can make better decisions on business initiatives, risk-reduction strategies, and the impacts of compliance regulations like the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act (PIPEDA), SEC cybersecurity guidance, and others. With a consistent approach to understanding cyber risk, you are empowered to expand use of third-party services, cloud technologies, and platforms.




## ENTERPRISE RISK ASSESSMENT SERVICES

Coalfire's enterprise risk assessment services help you understand the current cyber risks affecting your organization, security concerns with third-party service provider strategies, and opportunities to limit enterprise liability. These services deliver key insight on cybersecurity risks, recommendations on risk-reduction strategies, areas to improve operational and product protection from cyber incidents, and supporting data on reducing risks.

### Why choose Coalfire for an enterprise risk assessment?

- Our experts have a deep understanding of enterprise cyber risk, cloud and third-party service providers, deployment strategies, and security orchestration.
- We perform hundreds of cyber risk assessments across multiple industries for companies of all sizes.
- Our experienced consultants maintain various cybersecurity (e.g., CISSP, CCSP, CCSK) and cyber risk certifications (e.g., CRISC, OPEN-FAIR) and regularly contribute to cyber industry thought leadership initiatives.

DS_ERA_072320

## BETTER UNDERSTAND THE RISKS FACING YOUR ORGANIZATION.

**Learn about Coalfire's enterprise cyber risk assessment.**

Coalfire.com | 877.224.8077

COALFIRE

**About Coalfire**

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**