****

**Comprehensive board queries for cyber insurance effectiveness**

|  |  |  |
| --- | --- | --- |
| **Category** | **Key questions** | **Strategic focus** |
| **Coverage strategy** | What cyber risks are excluded from the current policy? | Risk identification |
|  | How do current coverage limits compare to potential breach costs in the industry? | Financial protection |
|  | What triggers could void coverage during a crisis? | Policy compliance |
|  | How does the current cyber insurance policy coordinate with directors and officers and E&O coverage? | Insurance integration |
| **Financial management** | What's the total cost of cyber risk (premiums plus uninsured exposure)? | Total cost of ownership |
|  | How do these premiums compare to industry benchmarks? | Market positioning |
|  | What ROI does the organization achieve from insurance-driven security improvements? | Value measurement |
|  | How would a major incident impact financial statements and credit ratings? | Business impact |
| **Risk management** | How does cyber insurance align with the organization's enterprise [risk appetite](https://www.techtarget.com/searchsecurity/definition/What-is-risk-appetite)? | Strategic alignment |
|  | What security controls are required to maintain our coverage? | Operational requirements |
|  | How does the organization measure and report cyber-risk maturity to insurers? | Performance metrics |
|  | What's the plan if cyber insurance becomes unavailable or unaffordable? | Contingency planning |
| **Operational oversight** | Who has the authority to make decisions during a cybersecurity incident? | Governance structure |
|  | How quickly can employees access insurance-provided incident response resources? | Crisis management |
|  | What documentation must be maintained to ensure successful claims? | Compliance management |
|  | How does the organization validate that its security controls meet insurer requirements? | Audit and verification |
| **Market intelligence** | How are cyber insurance terms and prices evolving in the industry? | Market awareness |
|  | What emerging risks might not be covered by current policies? | Risk planning |
|  | How do peer organizations structure their cyber insurance programs? | Competitive benchmarking |
|  | When should the organization consider [captive](https://www.cybersecuritydive.com/news/marsh-group-captive-cyber-insurance/711246/) or alternative risk transfer mechanisms? | Strategic options |
| **Regulatory compliance** | How does the organization's cyber insurance support SEC cybersecurity disclosure obligations? | Regulatory alignment |
|  | What cyber insurance documentation must be maintained for regulators? | Compliance documentation |
|  | How do state privacy laws affect coverage needs and requirements? | Legal compliance |
|  | What's the difference in reporting obligations to insurers as opposed to regulators? | Stakeholder management |
| **Claims readiness** | What scenarios trigger a cyber insurance claim? | Incident planning |
|  | How does the organization optimize the chances of full claim payment? | Recovery optimization |
|  | What's the backup plan if claims are denied or disputed? | Risk mitigation |
|  | How long does claims resolution typically take in the organization's coverage areas? | Business continuity |
| **Performance measurement** | What [key performance indicators](https://www.techtarget.com/searchbusinessanalytics/definition/key-performance-indicators-KPIs) require tracking for cyber insurance program effectiveness? | Success metrics |
|  | How does the organization measure the business value of its cyber insurance investment? | ROI assessment |
|  | What benchmarks help evaluate the organization's program against industry standards? | Comparative analysis |
|  | How often should the organization reassess its cyber insurance strategy? | Governance |