CFO Focus

Top of mind issues confronting the CFO

Issue #4: Cyber risk

CFOs are seeing their role continue to evolve and become more complex. That means keeping up with today's most pressing issues can be a challenge. KPMG created this series to provide cross-functional updates on the top-of-mind issues facing CFOs. This report includes information on trends and topics collected from discussions and interactions between KPMG professionals and the CFOs at some of our client companies. It also provides related resources on the topics as they pertain to the CFO and the finance function.

Cybersecurity and IT budgets

Companies increasingly recognize the value of all types of data—not just the data related to their customers or business partners. The downside is that this value hasn't gone unnoticed by hackers, and operational data is increasingly becoming a target of cyber-attacks. Accordingly, cybersecurity accounts for a greater part of corporate budgets than ever before. Cybersecurity is still largely seen as an IT expense. But while overall IT budgets tend to remain flat, the portion dedicated to cybersecurity is steadily rising and now commonly receives 8-12 percent of the IT budget.

Typically, boards need to be invoved to secure the necessary investment in cybersecurity. In many cases, the weight that an organization gives cybersecurity determines how often it is reported to boards. Most CFOs that KPMG has met with have shared that they report on cyber risks on an annual basis, others say they may present to their board 2 or 3 times a year. Conversations around cybersecurity tend to take place

Conversation guidance for budget planning and board governance conversations:
Board conversations around cybersecurity are much more successful when the topics relate to business strategy.

Understand the evolving risks faced by organizations:
Discusssion of cybersecurity protection is often heavily focused on consumer-related data. Operational data breaches are just as prevalent yet often less publicized. Operational risks typically refer breaches that have consequences affecting the confidentiality, availability, or integrity of information or information systems.

For example, IT disruption, data compromise, and regulatory risks.

Prevention, response, and mitigation plans must focus on more than just protecting your organization's brand; they must focus on protecting your operations and infrastructure.

Focus less on prevention of cyber risks and more on detection and response plans:
Security and data breaches are inevitable. That's why organizations should be more focused on improving their ability to detect and respond to an attack. These efforts should include:

- Breach simulations
- Scenario planning
- Tabletop exercises

Practice defensible cyber hygiene:
Companies must take and document the necessary prevention steps to protect against the legal implications of a cyber breach.

within audit committees or with entire boards, but a small percentage of companies, particularly those that are more data-sensitive, are moving toward establishing a board technology committees.

What are CFO's asking KPMG:

- What could be at risk within my organization, particularly in times of innovation, disruption, or fast growth opportunities?
- How can I get my technology teams to think in terms of risk mitigation as opposed to technology adoption?
- What are some leading practices for benchmarking the effectiveness of cyber security efforts and budgeting?
- How are organizations budgeting for cyber risk to ensure all stakeholder concerns are addressed, and how should we structure governance?
- What is the right frequency for communicating cyber risk issues and mitigation plans to the board? Is it time for the board to develop cyber risk committees?

Anthony Buffomante
Global Co-Leader and Americas Leader, Cyber Security Services
KPMG LLP
abuffomante@kpmg.com

Area of Expertise:
Cyber Strategy and Risk

"A major trend that is currently driving up cyber budgets is the explosive growth and value of the data being collected by organizations across all industries. Not just the data of customers or business partners, but the data driving operations and, in turn, driving strategic decisions. KPMG is seeing the risk of cyber-attacks aligned with this operational data growing significantly."

Cyber risk

Cyber risk has grown into a top concern for CFOs. Several high-profile cyber-attacks over the past year have raised awareness of cyber risk within organizations and caused senior leadership to take note of the threat that cyber-attacks pose. Interest in cyber security at the board level has increased the need for CFOs to communicate cyber risks to board members. Many CFOs give a comprehensive risk presentation to their board once a year that includes cyber risks. Other CFOs give presentations on cyber risk separate from broader ERM discussions. KPMG noted that an annual board briefing on cyber risk is becoming common among its clients, with the conversations commonly focused on cyber risk hygiene, adaptability (e.g., can a cyber risk program adjust to changes in the market?) and cyber risks within a business's ecosystem. KPMG has developed a framework for facilitating cyber security discussions between executives and boards. The framework is comprised of six elements: security leadership, human capital training and awareness, information governance, crisis response, regulatory and compliance, and technology operations.

Greg Bell
Principal, Global and U.S. Cyber Strategy Lead for KPMG
rgregbell@kpmg.com

Area of Expertise:
Cyber Strategy and Risk

"Cyber is much more about your company's business strategy and innovation plans than about technology architecture…We're doing business differently. It's very rare that all of a company's business functions exist within their own walls: Supply chains, business partners, and outsourcing relationships are all handling the company's critical data, including customer data. How do we protect that information and ensure that we are providing due care?"

The rise of cyber risk has created the need to companies to carry cyber insurance. Several members shared concerns about the limited offerings in the cyber insurance industry. Some standard coverages are emerging (e.g., breach remediation, business interruption, etc.) but many uncertainties remain as to what exactly cyber security covers. Areas where cyber insurance overlaps with other coverage also raise questions about how cyber insurance works (e.g., if a vehicle is attacked, is that covered by the auto policy or cyber insurance?) One member shared their challenges in obtaining cyber insurance to cover not only their legacy businesses, but a recent acquisition as well. The insurance for the new business needed to be in place on the day of the transition and cover issues that arise from times prior to the acquisition.

Enterprise risk management (ERM)

By guiding their organizations through ERM frameworks, appointing CROs and increasing cross-functional cooperation, CFOs are leading ERM efforts at their organizations. Many CFOs recognize the value of having a dedicated risk officer and either created or refreshed the role of the CRO. Some organizations regularly changes CROs as part of their ERM program. In many cases, the CRO reports to the law department, creating a hybrid risk management structure encompassing Legal and Finance. In other cases, CROs connect with senior leaders across the enterprise, providing a broad risk perspective to ensure that it is being mitigated appropriately.

What are CFO's Asking KPMG?:

— What should our focus be with respect to cyber risk?

— What are leading practices for risk reporting?

— Is cyber insurance something that should be part of our risk plan?

— How are leading organizations mitigating the risk pertaining to the current business climate and associated legislative/regulator/economic uncertainty?

Related KPMG resources

— The new mindset in cyber security: The board lens

— Cyber security from the front lines: Board oversight framework

Contact us

P. Scott Ozanus
Deputy Chairman and
Chief Operating Officer
KPMG LLP
T: 212-909-5571
E: psozanus@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia