Pearl Meyer

ASK THE EXPERT INTERVIEW | AUG 2024

Should Executive Pay Be Linked to Cybersecurity?



Aalap Shah

MANAGING DIRECTOR

Earlier this year, Pearl Meyer was approached by CNBC for commentary on Microsoft's announcement that it would include a successful cybersecurity strategy in its executive compensation plan. Managing Director Aalap Shah talked with the outlet more generally about this concept and if or how it might apply to other companies. The Q&A below is from a subsequent internal interview with Shah and Pearl Meyer's CIO Chad Flynn.

Q: How would an executive team—or the c-suite—exert relevant influence over the CIO, who is ultimately responsible for cybersecurity?

Aalap: As an executive compensation consultant, thinking about this from the aspect of building cybersecurity so directly into incentive plans, I question if you can have true or total accountability for something like this at the executive level. But if the overarching impact of the metric guides you to think about your business with the metric in mind, then it has a measure of influence. It's similar to having safety metrics for the executives at a manufacturing or energy company.

Chad: My view, as a CIO today, is that there are several indirect ways. Budgeting allocation—or withholding—is the domain of the CFO and can have a big impact on what the CIO is able to fund in terms of staffing, infrastructure, and proactive measures. A CHRO can have outsized cultural impact if they are leading the HR function in a way that helps hold the workforce accountable for the corporate IT policies meant to safeguard data. In short, there are certain action cases where the executive team can either broadly handcuff or broadly empower a CIO trying to do their best at keeping the organization and its clients and customers safe.

But there are clear examples of data breaches or cyber-attacks that can irreparably harm a company's reputation or halt its operations, and those can be completely outside the control of the executive team and the CIO. It comes down to building a culture of security.

And you are only as secure as your weakest link.

Q: A director or CEO might ask what happens if there's a failure and it's clearly not a result of either the executives' action or inaction? What would the compensation committee do about the incentive metric in that case?

Aalap: This specific idea is so new that we just don't have precedent for guidance, but it might be analogous to something like Covid. For instance, in some companies, everybody was doing everything right but an out-of-nowhere happening had massive, unexpected, and uncontrollable influence on financial metrics. Do you use discretion in that case, or do you hold fast to the plan? That's a philosophical question, but given how uncertain things can be of late, I would actually advise compensation committees to game-plan these kinds of scenarios, whether or not it relates to a cyber goal or some other more traditional metric.

It will be interesting to learn if the metric Microsoft has put in place is binary—either you get it or you don't—or if it is leveraged in some way that recognizes levels of achieved performance.

Chad: That's an interesting angle. From my perspective, an all or nothing approach might not make as much sense as something more gradient. If an employee has a malware situation on their individual device that is properly quarantined and that's as far as the incident goes, the CIO will definitely know about it, but the rest of the executive team will likely not. However, it technically is a breakdown in security. On the other hand, a ransomware situation that shuts down a hospital, for example, is clearly going to have effects far beyond the IT team or even the organization itself as it will impact providers and patients. We have recently seen how catastrophic one lapse can be with the global security software failure. And is that a cyber failure or is it a supplier and product failure?

Q: How are you talking with clients when they ask about this and if they should do something similar to what Microsoft has done?

Aalap: It's certainly unique and has gotten a lot of attention. Rather than trying to figure out if you should follow suit immediately or dismiss the idea, I suggest talking through the impact of cybersecurity to your business.

Recent history seems to suggest that managing through uncertainty is our new normal. Given this, it may be worthwhile for committees to consider adding a modifier to their incentive program to drive greater accountability when unforeseen events occur. In practice, the modifier could adjust the formula-driven incentive payout by plus or minus 10 to 20 percent and be compromised of a scorecard that includes metrics that are critical to

the organization’s sustainability, like cyber-security.

When the questions about ESG metrics began popping up, our fundamental guidance was that any factor included in an incentive plan must be material to your business. That holds true for financial and non-financial metrics, and it holds true here. Bigger picture, I think what we may begin to see is more organizations recognizing—especially after the global issue in late July—just how significant and material cybersecurity is to their operations and overall business strategy.

About the Author

Aalap specializes in executive compensation strategy—governance, pay-for-performance, and incentives—helping companies align business, people, and compensation strategy for effective programs.

About Pearl Meyer

Pearl Meyer is the leading advisor to boards and senior management helping organizations build, develop, and reward great leadership teams that drive long-term success. Our strategy-driven compensation and leadership consulting services act as powerful catalysts for value creation and competitive advantage by addressing the critical links between people and outcomes. Our clients stand at the forefront of their industries and range from emerging high-growth, not-for-profit, and private organizations to the Fortune 500.