Deloitte.

6-minute read

Incorporating cyber security in executives' incentive plans

Current state AEX & AMX companies:

- **3** companies, (IMCD, Randstad & Wolters Kluwer) operate cyber security metrics as part of the non-financial metrics in their Short-Term Incentive Plan ("STIP"). These metrics are specified as follows:
  a. Enhancing cyber security;
  b. Achieving world-class digital security;
  c. Indexed cyber security score target.
- Wolters Kluwer's Indexed cyber security maturity score is based on a company-wide program designed to maintain and advance cyber security, assessed annually by a third party.
- **None** of the companies operate a cyber security metric in their Long-Term Incentive Plan ("LTIP").

Market practice UK (FTSE 100 & 250):

In the UK, the topic is slightly more mature:

- **13** listed companies, active within various industries, have a cyber security metric in their STIP, part of the non-financial metrics.
- Targets are specified as follows:
  - Enhancing cyber security strategy;
  - Improvement cyber security program;
  - Mitigating firm's cyber risks;
  - No data breaches.
- **1** company (Standard Chartered) has included a cyber security metric in its LTIP, part of strategic metrics.
- This target is specified as follows:
  - Successfully deliver milestones within the information and cyber security risk management plan.

Companies increasingly linking cyber security with executive compensation

Digital transformation and cyber risk

Many organizations are transforming into digital businesses, using emerging technologies to change business models and create new revenue streams and value propositions. It is clear that digitalization brings considerable benefits to organizations.

However, the risk associated with digitalization (i.e., cyber risk) is also increasing proportionally and has become one of the most critical risks for almost every organization in any industry. Cyber attacks can disrupt a company's business operations and may result in downtime, data breaches, revenue loss and reputational damage.

This digitalization trend emphasizes the importance of becoming cyber resilient. For organizations to thrive through digitalization, they should be ready to deal effectively with high-impact events or crises, being an expected one, such as a reorganization or an unexpected one, like fraud, a cyber attack, or a technical breakthrough.

"This digitalization trend emphasizes the importance of becoming cyber resilient"

Ownership starts at the top

As an Executive Board, proper governance includes leading and investing in a security culture, challenging the organization's preparedness, and acting as a security ambassador for employees and clients. The only effective strategy to preserve and sustain business in the medium-long term is by prioritizing cyber resilience.

What gets rewarded gets done

Despite increasing awareness of cyber security risks disclosed in most companies' risk management sections of the annual reports, very few (large) organizations currently include a link between cyber security performance and executive compensation.

Because of the vital importance of cyber security and the increasing number of cyber attacks worldwide, including cyber security related metrics/KPIs in incentive design is worth careful consideration. Especially as incentive design (if structured in the right way) has proven to be a powerful tool in driving executives' behaviors.

Moreover, the inclusion of cyber security performance metrics in incentive plans sends an important signal to executives, employees, investors and wider stakeholders. Of course - as with any metric – it is critical that the Remuneration Committee ("RemCo") ensures that they have enough flexibility to safeguard against rewards for failure and seeks external assurance around target-setting and performance out-turns.

Deloitte.

6-minute read

Cyber security metrics as part of ESG reporting?

Should cyber security be part of ESG reporting?
Reporting on the ESG performance of an organization is becoming increasingly important. Cyber security, however, is usually not included. Less than 2% of large organizations published ESG goals (ESG) related to cyber security in 2021, where a shift is expected to approximately 30% by 2026 according to research by Gartner.

There are many reasons to include cyber security in ESG reporting:

- *Threat to business value.* Ransomware attacks have increased in number, and the impact is typically larger on more complex and sophisticated targets. Threat actors have changed their tactics by shifting from large-scale, programmed attacks to targeted, multi-faceted, bespoke attacks often enabled by readily available malware tooling. Unfortunately, this means the attacks are increasingly common, more targeted and harder to recover from than ever.

- *Threat to society*. Data breaches from a company's digital environment can put individual customers' security and financial stability – and employees' personal data at risk. Cyber attacks affecting the availability of critical infrastructure, such as the Colonial Pipeline attack in the United States, broadly damage society and businesses.

"Data breaches from a company's digital environment can put individual customers' security and financial stability – and employees' personal data at risk"

- *Responsible business/corporate governance*. Operating as a responsible business obliges organizations to be transparent about how resilient the organization is to cyber attacks. Cyber risk metrics may reflect an organization's attitude and consequently drive behavior on how to protect themselves against a future breach. The Executive Board must identify who is responsible for cyber security and determine reporting requirements to the Executive Board.

- *Availability of a framework*. An organization requires a framework to be able to report cyber resilience. Industry-standard frameworks are being developed by established third parties (e.g., Global Reporting Initiative [GRI], Sustainability Accounting Standards Board [SASB] and the European Sustainability Reporting Standards [ESRS]). Such frameworks will enable organizations to include cyber security goals and metrics in ESG reporting and demonstrate commitment to cyber resiliency.

Spotlight on ESG & remuneration

- An effective Environmental, Social and Governance (ESG) strategy has rapidly gone from being a 'nice-to-have' to a necessity. Companies, investors and wider stakeholders increasingly recognize that an ESG strategy intrinsically links to future business resilience, and can positively impact many areas, from attracting talent and engaging employees to improving financial performance.
- The actions of business executives are seen as critical in driving the ESG strategy. Although there are mixed views around the effectiveness of incorporating ESG metrics in executive compensation, it can be a powerful tool for driving leadership behaviors if structured in the right way, and linked to transparent and quantifiable performance metrics.
- In the Netherlands, we observe that most large listed companies already have incorporated ESG in their executive incentive plans, mainly as a basket/scorecard or stand-alone metric, and we expect more companies globally to move toward linking incentive plans with ESG performance and specifically sustainability goals.

Deloitte.

6-minute read

How to incorporate cyber security in executives' incentive plans

There are different ways to link cyber security with executive compensation

Cyber security in incentive plans
Before incorporating cyber security in executive compensation, it is essential that cyber security is embedded in the company's broader corporate strategy. If the cyber security conversation would start or be led by the RemCo, it implies an absence of a foundation.

If cyber security is to be included in executives' incentive plans, executive compensation must be linked to the cyber security strategy. This requires clear objectives, time-based targets and KPIs that build on the corporate cyber security strategy. To maximize impact, the collection of sufficient cyber security data and overall cyber security strategy communication in external disclosures are crucial. Finally, cyber security metrics should continuously be monitored, developed and reviewed to ensure they remain material to the strategy.

"To maximize impact, the collection of sufficient cyber security data and overall cyber security strategy communication in external disclosures are crucial"

Key considerations for RemCos
Making the right decisions when linking cyber security with executives' compensation can be very challenging for RemCos. We often observe challenges to reach internal consensus and/or absence of specific knowledge in this field of expertise. Important areas of consideration are *performance metric selection*, *appropriate target-setting* and *disclosure and communication.*

Cyber security can be incorporated in incentive plans in various ways, such as including a cyber security metric as prerequisite for any pay-out, including it as part of a basket of metrics and/or including cyber security as a stand-alone metric. Actual cyber security metrics could, amongst others, be the average time to recover from a cyber incident, the total uptime of all digital systems during a period and/or what has been done to reduce vulnerabilities and risks – assuming the conditions defined in the previous section. In addition, it is of vital importance that the KPI(s) selected should be quantifiable and measurable.

We are here to help
Our multidisciplinary team, including executive compensation and cyber security professionals, understands the challenges around building cyber security into your company's incentive plan and defining specific cyber security metrics to include and measure going forward. We can help you to maximize the effectiveness of your incentive plan.

For more information – meet our experts:

Ferry Noordzij
Cyber & Risk Advisory
Tel: +31 6 13 76 03 29
Email: fnoordzij@deloitte.nl

Roel van der Weele
Executive Compensation
Tel: +31 6 29 66 61 29
Email: rvanderweele@deloitte.nl

Tom van den IJssel
Executive Compensation
Tel: +31 6 29 66 05 38
Email: tvandenijssel@deloitte.nl

Deloitte.