



The CISO and the Board: Partners against Cyber Crime

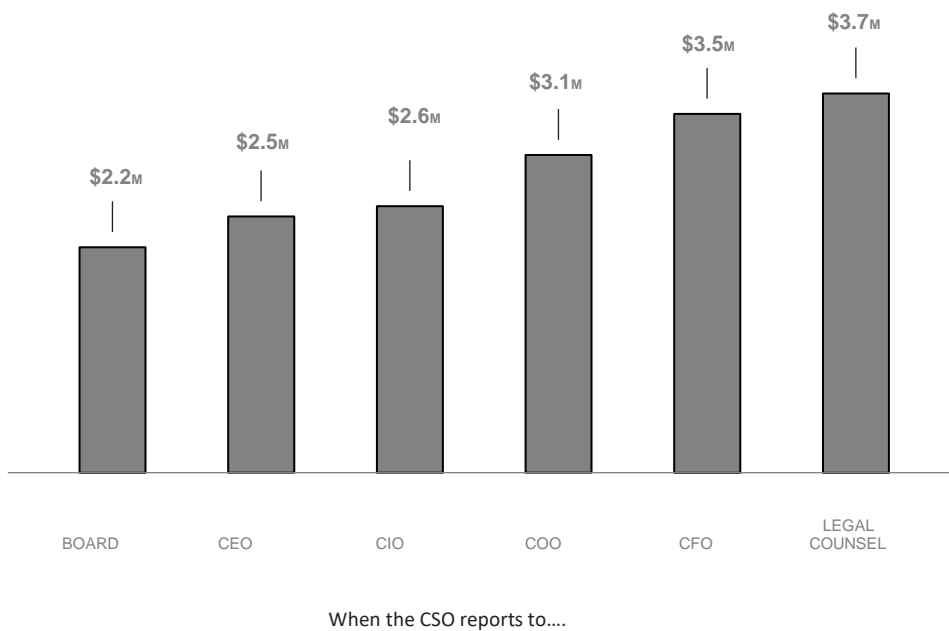
“United we stand, divided we fall” is an excellent motto when it comes to building a cyber safe organization.

While cyber security can't be 100% guaranteed, the risk of breaches drops considerably when the Chief Information Security Officer (CISO) has a strong working relationship with other department heads and – most importantly – the Board.

A recent **GSISS survey** shows that if the Chief Security Officer (CSO) reports to the Board, financial losses are lower.

Fig 1.

Average estimated financial losses from security incidents



As companies face mounting financial and reputational threats from hackers, criminal gangs and nation-state actors, the alliance between the CISO and the Board has never been more important.

So, how can these two partners build a strong working relationship?

The role of the CISO

Seek first to understand, then to be understood

Focus on the business issues

The CISO must understand the company's business priorities and how they are impacted by cyber security. A good Board will focus on how cyber security affects financial and operational performance, brand value and investor confidence. The CISO should explain how cyber safety fits with broader strategy execution and the business 'risk appetite.

Ensure integration

The CISO should work closely with the CEO and executive team to establish cyber security initiatives that support the overall strategic objectives of the company. The CISO who aligns plans and budgets to the company strategy is more likely to receive funding and support.

Link security to costs

Boards like return on investment (ROI) information. In presentations, show the estimated savings when a cyber-attack is thwarted, or the ROI of faster breach containment. If you're requesting support or funding, explain the potential losses and demonstrate the likely ROI.

Look ahead

Most of the information a Board receives is nearly two quarters old. The CISO's team should present forward-looking insights, indicating both upcoming opportunities for greater security as well as potential threats. Extrapolations and predictive analytics are useful in helping Boards plan and make better recommendations.

Educate

Boards might have one or two members with technical backgrounds, but it's likely that most members won't be experts in cyber safety issues. Don't try to teach them everything at once but do use every opportunity to educate them on the importance of cyber security to the business.

Use a dashboard

Visuals and graphics are great for condensing information in an easy-to-understand way. As always, make sure your oversight is forward looking and focuses on future risk, strategy and ROI.

Break down silos

Cyber security is a team sport. It's the CISO's responsibility to ensure that all functions and departments understand their individual and collective roles in cyber safety. In many organizations, poor cross-functional communication and lack of cooperation creates unnecessary risk.

Ask: How can I better support you?

At the end of every CISO presentation to the Board, it's useful to ask how the cyber security team can better support the business. This often elicits important insights.

The role of the Board

A two-way partnership

Do your homework

Typically, only a few board members are tech savvy and engage in discussions about cyber security – while the rest don't feel confident enough. We strongly suggest that every board member gains a basic understanding. Books such as [Cyber Security for Dummies](#) or online resources such as [CyberVista](#) are good places to start.

Demand an enterprise approach

Ensuring cyber security is too big a job for any one function. To fully protect the company, the Board should ensure that the CEO encourages and supports the functional heads to work with the CISO to make sure all employees have the skills, knowledge and understanding of safe cyber practices and breach responses.

Culture and employee engagement

A majority of cyber breaches have a human fingerprint and as a consequence, Boards are increasingly being asked for oversight on corporate culture. The Board should request that the CISO presents information on how culture and employee engagement impact cyber security.

Ask: How can the Board better support you?

While a good Board discussion will address many questions concerning cyber security and future risks, always ask the CISO what help they need. This often leads to fruitful conversations.

An Important Partnership

*“Alone we can do so little;
together we can do so much.”*

— Helen Keller

Strengthening the working relationship between the Board and the CISO is in everyone's best interests. Since enterprise risk is a key function of the Board, we encourage the Board Chairman to make this partnership a priority