KINGSLEY GATE
PARTNERS

# Don't leave Cyber for your next Chief *Scapegoat* Officer

Identifying the best cyber risk response strategy for your firm

The starting gun has fired. According to Gartner, 50% of the C-suite will have cyber risk related performance requirements built into their contracts by 2026. Cyber is finally being viewed from the perspective of organizational risk management rather than an IT issue. Get ahead of the curve and begin with a robust cyber risk assessment strategy and avoid scrambling to identify your next Chief Scapegoat Officer.

Most Boards of Directors come from non-IT backgrounds. Only a fraction of S&P 500 independent directors have experience leading Cyber Security, IT, Software Engineering or Data Analytics[1]. That 4% is also confined to Tech centric companies. Consequently, the demand for Cyber and Security risk backgrounds for board members is dramatically increasing.

Cyber should be number one on the agenda and covered at least once a quarter. Cyber is a board level concern. You may not be able to fully satisfy the board but you can make sure they're not dissatisfied in the event of an attack.

Essentially you want your executive audience to not think negatively of your cyber security program.

# How can you ensure that?

## What CISOs can/must do

Currently, there is a mismatch between a board members background and a CISO's background, which extends to a delta in language and terminology.

As a CISO, you should never get too technical with your leadership team as they will just tune you out. Instead communicate by telling stories and demonstrate how other companies in similar industries have encountered Cyber Security issues and what they did about them successfully and unsuccessfully. Another point would be to demonstrate the changing threat landscape. Highlight the reputational, financial regulatory and legal risk at stake.

What you want is the board to hold Cyber Security culture at the top of their agenda. Get a formal declaration of support from the top and your handle on your scope of authority will increase.

Articulating a cyber security strategy is critical as a CISO. But it should also fall to the Board to set the right security culture.

# Building a Robust Cyber Risk Framework

A successful Cyber Risk Framework should cover the following key elements.

## Cyber Risks and Responses:
## lay out the organisations top risk vulnerabilities such as ransomware, data privacy, third party compromises, email compromise and phishing.

- As a CISO, demonstrate what you're currently doing to mitigate the risk, the likelihood for it to occur, the impact in case it occurs, what the function is doing in order to prevent it, and provide a scenario of how much a breach could cost to fix.

- Identify the top cyber risks and demonstrate the responses to each one. Acknowledge the existence of risk and response rates. If the executive leadership team isn't satisfied this is a good opportunity, highlight a robust cyber risk framework with more resources or security vendors to demonstrate how the risk can be significantly reduced or automated thereby creating a sound business decision.

## Tactical Cyber Metrics:
## Analyse the threats, status, trends and goals.

- Technology - how fast it takes to make patches and what can be done to escalate them.

- People - record click and reporting rates. Analyse phishing exercises across industry peers to see how you compare.

- Process 3rd party risk through pen testing. Identify what percentage of critical applications performed adequately during disaster recovery and business continuity.

- Environment – what lies outside of the organization that you can't control but it still has a significant impact. These could be new cyber laws, fraudsters, and malicious actors.

## Roadmaps

- Identify high profile programs and strategic initiatives. Articulate and demonstrate a solid plan over the next few years that can be reviewed in stages.
- Provide a big picture over the next three years based on the current priorities. This can include launching a bug bounty program, upgrading firewalls, botnet protection tools, vulnerability management, custom courses and in house training.

## Cyber Maturity Assessment

### Independently measure the effectiveness of the entire cyber program.

- Benchmark the program by hiring an outside independent auditing company to assess how you're performing across the competitive landscape with your peers.
- Action insights from the independent assessment on top activities to improve scoring measurements across top priorities.
- Provide a timeline on when they will be improved or fixed.

## Conclusion

Your goal as a CISO is to keep the executive leadership team well informed and hold C-level executives accountable for funding and maintaining your cyber security initiatives.

The Board, too, must ensure the successful integration of cybersecurity measures for the benefit of all involved shareholders[1]. Solidarity, transparency, and trust are critical across functions in order to be able to respond swiftly and decisively in today's evolving threat landscape.

[1] Cybersecurity: What role does the board play?

*Authored by*

Vanya I. Mackay

Vice President

KINGSLEY GATE
PARTNERS