KnowBe4

10 Best Practices for CFOs to Communicate Cyber Risk Strategies to the CEO and Board

As cybersecurity takes on increased importance across industries, CFOs are in a unique position to bridge financial expertise and cyber risk management. When communicating with the CEO or board, it's crucial to convey how cybersecurity initiatives align with broader business objectives, positively impact risk and outline cost-benefit analyses. **Here are ten best practices to help CFOs effectively articulate cyber risk strategies.**

1. Use Business-Centric Language

When discussing cyber risk, avoid technical jargon in favor of terms that are business-relevant. CEOs and board members want to understand cyber risk as it pertains to business outcomes, so describe threats in terms of potential impacts on revenue, compliance and reputation. Frame cyber risk as a financial and operational concern, rather than a purely technical one. For instance, describe ransomware in terms of possible business downtime and revenue loss rather than focusing on malware types or encryption.

2. Highlight Cybersecurity's Role in Compliance and Regulation

Compliance with cybersecurity regulations (e.g., GDPR, CCPA, and SOX) can directly impact a company's financial health. CFOs should emphasize how the cybersecurity program aligns with regulatory requirements, avoiding fines and protecting the organization from legal liability. Articulate how non-compliance could lead to fines or operational limitations, and contrast this with the cost of compliance initiatives, reinforcing cybersecurity as both a compliance need and a financial safeguard.

3. Present Quantifiable Financial Impacts

Quantify the potential financial impact of cyber risks and mitigation efforts whenever possible. CFOs should work with cybersecurity teams to estimate costs associated with various risks, such as data breaches or ransomware incidents, and link them to potential financial losses or regulatory fines. This approach allows board members to grasp the importance of cybersecurity in terms of dollars and cents, making it easier to evaluate cyber initiatives alongside other financial considerations.

4. Connect Cyber Risk to Strategic Business Objectives

Position cyber initiatives as enablers of core business goals such as innovation, market expansion or customer trust. For example, if a company is looking to expand into a region with strict data privacy regulations, outline how investments in cybersecurity will support that growth by ensuring compliance. This helps the board understand cybersecurity not as a cost center but as a necessary part of the business's strategic foundation.

5. Establish Clear Metrics and KPIs for Cybersecurity Initiatives

Use key performance indicators (KPIs) to track cybersecurity improvements and investments. Metrics like "time to detect and respond to incidents," "vulnerability remediation rate," or "number of phishing simulations passed" can illustrate the impact of cybersecurity efforts. CFOs can further enhance these metrics by tying them to financial outcomes, such as reduced incident costs or lower insurance premiums, demonstrating cybersecurity's value over time.

6. Demonstrate Cost-Benefit Analyses for Cybersecurity Investments

CFOs should apply the same rigorous evaluation to cyber initiatives as they would for any other investment, presenting ROI calculations or cost-benefit analyses for proposed cybersecurity measures. Explain the projected ROI of cybersecurity investments in terms of risk reduction or avoided costs. For example, compare the cost of implementing multi-factor authentication (MFA) with the potential financial losses from a data breach, underscoring how preventive measures can be financially beneficial in the long run.

7. Leverage Scenario Analysis for Potential Cyber Incidents

To help the board visualize the impact of cyber threats, CFOs can present scenario-based analyses, such as "if a ransomware attack occurs" or "if our customer database is breached." Describe how these scenarios could affect the company's revenue, stock price and reputation, and discuss contingency plans to mitigate these risks. Scenario analysis brings cyber risk to life for the board, giving them a realistic view of possible outcomes and the efficacy of planned countermeasures.

8. Benchmark Against Industry Standards and Peers

Boards are often concerned with how the company measures up to industry standards. CFOs should leverage benchmarking data to show where the organization stands in relation to competitors and industry best practices. For instance, if other companies in your sector have adopted a certain cybersecurity framework, highlight how your company is aligned or discuss plans to catch up. This puts the company's cyber strategy in a competitive context, which resonates with leadership focused on industry standing.

9. Provide a Transparent View of Cyber Insurance Coverage

Many boards now consider cyber insurance as part of the risk management strategy. Outline what the company's cyber insurance covers and any gaps that could lead to financial exposure in the event of a major cyber incident. Be transparent about any limitations in coverage and communicate how insurance fits within a larger risk management plan. This helps the board understand insurance as one part of a broader, layered approach to cybersecurity rather than a complete safeguard.

10. Establish and Communicate a Regular Reporting Cadence

Cyber risk management should be an ongoing conversation, not a one-time report. In conjunction with your CSO/CISO, establish a regular cadence for cyber risk reporting, using dashboards or executive summaries that highlight key metrics, emerging risks and status updates on cyber initiatives. Regular reporting keeps the board informed and engaged, making them more likely to support cybersecurity funding. It also establishes cybersecurity as a critical, continuous business focus rather than a sporadic concern.

Conclusion

CFOs play a crucial role in ensuring the board understands both the financial implications and strategic importance of cybersecurity. By adopting these 10 best practices, CFOs can communicate cyber risk management effectively, helping boards make informed decisions that align with the company's goals and risk tolerance. With clarity and transparency, CFOs can demystify cybersecurity for leadership, positioning it as an essential, strategic investment.

Learn More About What KnowBe4 Can Do For Your Organization

Additional Resources

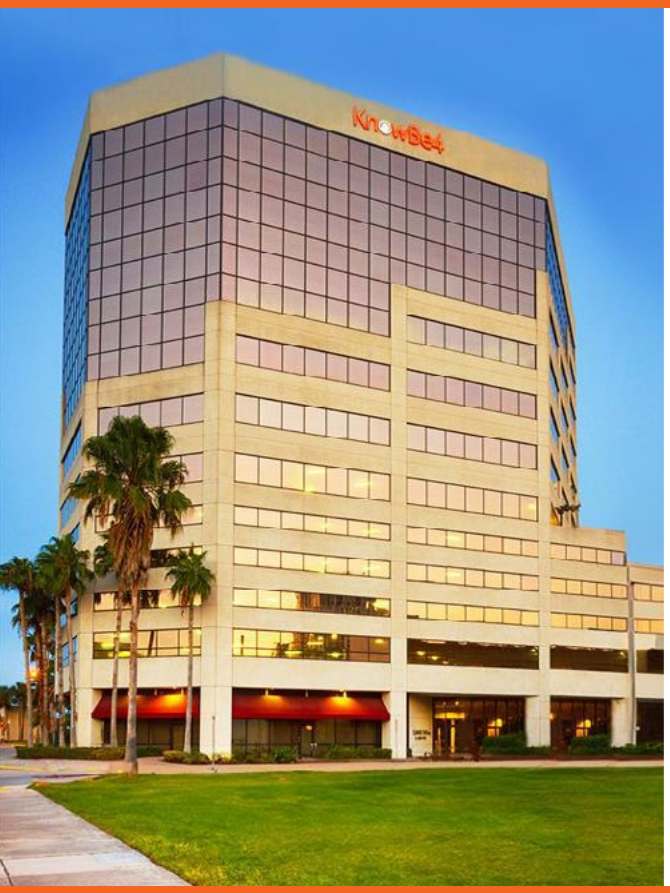
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E09K01