ISACA

# 10 Tips
## for Talking Cybersecurity With Your Board

A recent study from global technology association ISACA found that 87 percent of C-suite professionals and board members lack confidence in cybersecurity initiatives. How can you talk to your board in a way that builds trust and gains buy-in?

### 1 Know your organization's cybersecurity risks.

Ensure that you've identified and documented all of the potential risks facing your organization. With strong communication and documentation, it will be easier to obtain support for risk mitigation efforts.

### 2 Communicate your organizational risks effectively.

Understanding your risks is good—but being able to effectively communicate them to stakeholders is better. Don't just tell leadership what the concerns are—provide context and illustrate potential effects in terms of financial impact or damage to your brand reputation. Ensure that you've identified and documented all of the potential risks facing your organization. With strong communication and documentation, it will be easier to obtain support for risk mitigation efforts.

### 3 Know your security controls.

Understand what security controls are in place within the organization, ensure they are documented and understand their efficacy. Don't forget, security controls can take many forms, from technical tools to organizational processes such as incident response plans, or people such as physical security guards.

### 4 Communicate security control needs.

Make sure that stakeholders are aware when a certain control needs more attention or funding. Gaining buy-in from leadership will ensure critical controls are maintained. Effective communication describing the security control needs to the board will help illustrate the importance of investing in these valuable preventative measures.

### 5 Show fiscal relevance.

Boards need to understand what kind of financial commitments are required to support a mature cybersecurity posture. Illustrating how cutting-edge cyber trends can impact the bottom line may be the make-or-break factor for board approval.

### 6 Communicate business impact.

Effectively articulate best- and worst-case scenarios to leadership. Providing this type of awareness will ensure that boards understand what is at stake, should an incident occur.

### 7 Have a plan.

Illustrate how changes made within an organization can increase organizational cyber maturity. Provide a roadmap, with concrete action plans and dates, to show how a stronger cyber stance is achievable. Document the risk mitigation efforts, explaining the reasoning for pursuing specific risks over others—remember, it is okay to only address certain risks, as long as they are directly applicable to your organization and are documented as such.

### 8 Illustrate improvement in cyber maturity.

Present growth over time to the board. Demonstrate how implementing previous controls made the organization more resilient. Make the illustration personal by focusing your lens on the specific needs of the organization. Contextualized improvement consistently outweighs abstract growth.

### 9 Encourage tenacity.

Over time, as an organization's cyber maturity increases, fewer catastrophic incidents may occur. Encourage the board to continue its dedication to staying cyber strong and maintaining funding and personnel. One effective method of encouragement is through continuous evaluation, demonstrating that the need for a strong cyber posture is constant.

### 10 Stay data-driven and transparent.

Even if the truth hurts, it is important that boards have an honest understanding of the organization's cyber maturity levels (or lack thereof). Only through transparency can they address cyber threats head-on.

ISACA's CMMI® Cybermaturity Platform makes cyber resilience—and more effective conversations with your board—possible. Aligned with leading security frameworks like NIST, its assessment generates a unique risk profile for your organization, prioritizes gaps in capabilities, identifies the maturity required to achieve your organizational goals, and recommends options to address the gaps. With this data in hand, ISACA's CMMI Cybermaturity Platform builds your board's confidence and trust by aligning strategic objectives with pragmatic insights into cybersecurity risks.

To learn more about the CMMI Cybermaturity Platform or schedule a demo, visit www.cmmiinstitute.com/cyber maturity.

ISACA