

# CYBER RISK IS A BOARD ISSUE: FROM "ARE WE SECURE?" TO "ARE WE PREPARED?"

According to research published in Harvard Business Review, 65% of Board directors believe their organization will face a material cyberattack within the next 12 months, and nearly half feel unprepared for a targeted attack. The Board's question is no longer whether the organization is secure. It is whether the organization is prepared.

## WHY CYBER BELONGS IN THE BOARDROOM

### **Cybersecurity is enterprise risk.**

A serious cyber event can affect financial performance, operations, reputation, stakeholder trust, regulatory standing and long-term value. NIST now places cybersecurity governance alongside financial and reputational risk within enterprise risk management.

### **The financial exposure is real.**

Stolen funds, business interruption, legal costs, regulatory penalties, recovery expenses and reputational damage can quickly become a material financial issue that reaches the Board level.

### **Your risk extends beyond your walls.**

A disruption at a vendor or business partner can become your operational crisis, even when your own systems are working normally.

### **Oversight is now a governance expectation.**

SEC rules require public companies to disclose how their Boards oversee cybersecurity risk, which reflects a broader shift from treating cyber as an IT function to treating it as a governance responsibility.

## WHAT THE BOARD'S ROLE IS, AND ISN'T

### **Risk oversight, not technical oversight.**

Directors don't need to become cybersecurity experts. They need to understand the organization's most significant exposures, whether those risks are acceptable and whether management is ready to respond.

### **Start with what matters most.**

The conversation begins with critical operations, services, information, finances and reputation, not with technology.

### **Resilience matters as much as prevention.**

Beyond "Can we stop an attack?" the Board should ask "If something gets through, can we keep operating and recover quickly?"

### **Investment is a risk decision.**

For every cyber investment, the Board should understand what risk it reduces, what risk remains and whether that remaining exposure is acceptable.

## QUESTIONS?

Conner Strong & Buckelew's Center of Excellence closely monitors emerging threats and trends to support our clients. Please reach out to your account representative or call us at 1-877-861-3220 with any questions.

CONNER  
STRONG &  
BUCKELEW

## QUESTIONS EVERY BOARD SHOULD BE ASKING

1

Where are we most exposed?

2

Is our risk improving over time?

3

What remains outside our risk tolerance, and what are we doing about it?

4

What happens if prevention fails, and how quickly can we recover?

5

Which vendors or partners could disrupt our operations?

6

What decisions or investments do we need to make now?

## THE BOTTOM LINE

The Board doesn't need to know how the organization is protected. It needs to know what is at risk, how prepared the organization is, what could happen if prevention fails and what decisions are needed to stay resilient.

CONNER  
STRONG &  
BUCKELEW