NACD NORTHERN CALIFORNIA LEADERSHIP COUNCIL
INSIGHTS ON TOP NACD MEMBER CONCERNS

# Why Boards Must Prioritize Cybersecurity in 2025

As our systems become increasingly digitalized, their vulnerability to cyber threats also rises. Malicious actors are becoming more sophisticated, and recent incidents have shown that critical infrastructure is a prime target. This is a wake-up call for organizations to elevate their cyber governance maturity to prevent disruptions to essential services that communities rely on. Cyberattacks are inevitable; however, a robust cybersecurity strategy is essential for both preventing and addressing these threats.

## TRENDS & EMERGING ISSUES

1. The convergence of information technology and operational technology makes critical infrastructure vulnerable. GHD Digital research shows that the average annual rate of cyberattacks on infrastructure is growing at 125 percent.
2. The evolving cyber-threat landscape is dominated by nation-state actors, cybercriminal organizations, and insider threats. A combination of these adversaries' motives and employees' uninformed actions pose a formidable danger to systems, highlighting the need for comprehensive awareness and training programs.
3. The adoption of cutting-edge technologies for operations—IoT, cloud computing, and family of AI technologies—presents a double-edged sword. While these technologies enhance operations and management of assets, they also expose organizations to new threat vectors.

## CASE STUDY

GHD Digital's research shows that more than half of global infrastructure suppliers have experienced attempts to control and shut down their systems, the majority of which could not block the initial attack. Managing a data breach in critical infrastructure is estimated to cost an average of $5.5 million, surpassing the estimate for other industries such as retail, pharmaceuticals, and hospitality, where a breach costs $4 million. A high-profile example was the ransomware attack on the Colonial Pipeline, an American oil pipeline system carrying gasoline and jet fuel to the Southeastern part of the United States. This disrupted gasoline and other products along the East Coast, which led to fuel shortages and price hikes.

## IMPACT

Imagine this: no power, water, or access to essential services. This dire scenario seems far-fetched, yet recent events give credence to this possibility, especially when organizations operate without adequate safeguards. Compromised critical infrastructure can cause a chain reaction, leading to prolonged service disruptions, substantial economic losses, and social unrest. On an enterprise level, the data, assets, bottom line, and reputation of organizations are at stake. A cyberattack could lead to loss of data, revenue, and stakeholder trust. Companies could also incur safety, environmental, and legal damages.

GHD Digital

NACD NORTHERN CALIFORNIA CHAPTER LEADERSHIP COUNCIL

## HOW TO MITIGATE RISKS

- Demonstrate executive ownership and serve as advocates for a strong security culture, creating a top-down approach to protect data and systems.
- Adopt a well-structured cybersecurity strategy that is closely tied to business objectives and risk assessment to ensure that security investments are targeted where they matter most.
- Embrace security by design by embedding security measures from the outset instead of being bolted on later, minimizing weak links and reducing the likelihood of costly breaches down the line.

## QUESTIONS FOR YOUR NEXT BOARD MEETING

- How can we develop a solid cybersecurity strategy as part of the overall organizational strategy?
- How are we fostering a cybersecurity culture?

***"Proactive cybersecurity actions go beyond a box-ticking exercise; in a wider context, they are about ensuring that the backbone of our society remains resilient now and into the future."***

***— Kumar Parakala, President at GHD Digital***