ISACA | CMMI Institute — AN ISACA ENTERPRISE

THE BUSINESS IMPACTS OF A CYBERSECURITY CULTURE

Fewer than half of organizations say their security culture is very successful—yet most recognize the numerous benefits a culture of cybersecurity can bring, including a stronger reputation, deeper customer trust, and even higher profit. Global technology association ISACA and the CMMI Institute conducted a global survey on security culture, and key findings are below. For full results, visit www.isaca.org/cybersecurity-culture-study.

95% SAY THERE IS A GAP between the organization's desired and actual culture of cybersecurity

87% SAY ESTABLISHING A STRONGER CULTURE of cybersecurity would increase their organization's profitability or viability

FEWER THAN HALF

conduct **hands-on testing to train employees** on security awareness or best practices

THE CYBERSECURITY CULTURE GAP

How is the health of your organization's cybersecurity culture?

- 33% GOOD
- 22% FAIR
- 30% VERY GOOD
- 7% EXCELLENT
- 7% POOR

WHAT'S CAUSING THE GAP?

- ONLY 34% SAY EMPLOYEES HAVE A **solid understanding of their role** in the organization's security culture
- 20% SAY NO ONE IS PENALIZED for **not following** security policies/procedures
- 17% REWARD STAFF who **follow** security best practices/policies

Primary Factors Inhibiting a Strong Culture of Cybersecurity:

- 41% Lack of employee buy-in
- 39% Disparate business units (different styles, regions, cultures, etc.)
- 33% No set KPIs or business goals
- 29% Lack of funding
- 27% Lack of senior executive buy-in or understanding

CLOSING THE GAP

Primary Factors That Empower a Culture of Cybersecurity:

- CLEAR AND CONSISTENT POLICY 69%
- 60% EMPLOYEES FOLLOWING SECURITY POLICY
- 57% REGULAR SECURITY TRAINING, ESPECIALLY HANDS-ON
- 51% EMPOWERED CISO
- 43% EXECUTIVE CHAMPIONS WHO SPEAK UP FOR SECURITY

Top 3 Benefits Realized From Successful Cybersecurity Culture:

- 66% REDUCTION OF CYBERINCIDENTS
- 65% Strong customer trust
- 55% Better brand reputation