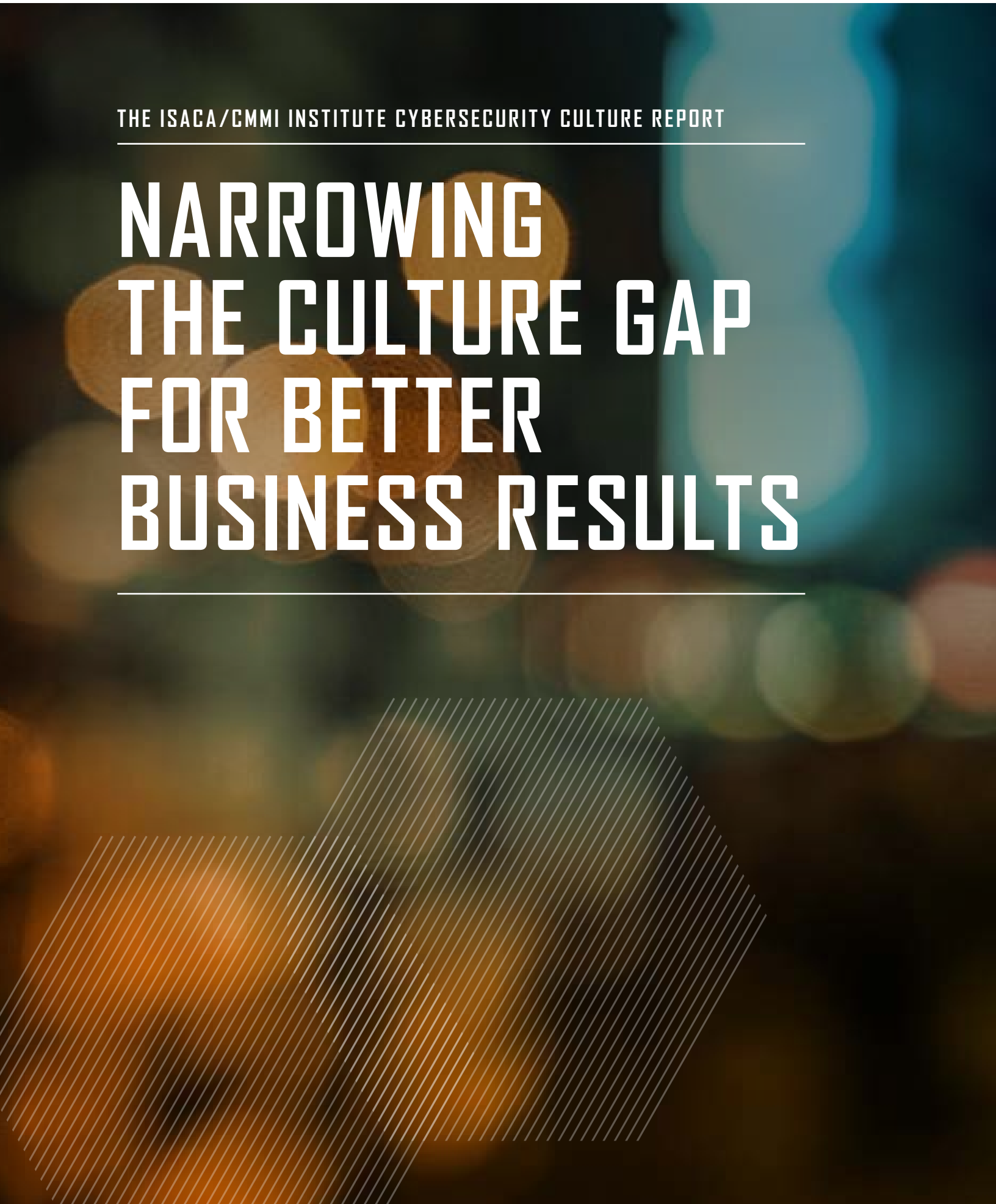
ISACA

CMMI Institute
AN ISACA ENTERPRISE



THE ISACA/CMMI INSTITUTE CYBERSECURITY CULTURE REPORT

NARROWING THE CULTURE GAP FOR BETTER BUSINESS RESULTS

Introduction

The human element is central to an organization's strategic management of its cybersecurity posture. Yet, initiatives to manage cyber defenses often rely on examples borrowed from the annals of warfare, with an emphasis on securing all boundaries and delivering a knock-out. As ISACA and CMMI Institute security experts[1] make clear, such old school tactics are no longer effective given the mutating nature of cybercrime and porous digital boundaries in our interconnected world.

According to World Economic Forum analysts,[2] successfully countering the skyrocketing number of cyberattacks requires a coordinated team effort. And, in the business environment, as documented by studies[3] from MIT Sloan School of Management and Carnegie Mellon University, effective high-performing teams are characterized by open communication, trust, collaboration and shared responsibilities among their members.

Likewise, in today's digital landscape, a cybersecurity program that has the active engagement and ongoing vigilance of an enterprise's entire team, top down and bottom up, will have more successful outcomes than an organization relying on a heavy-hitting technology fix or INTERPOL detectives to land a knock-out blow.

However, not every organization understands how to establish a workplace culture where security awareness and behaviors are seamlessly integrated into everyone's daily operations. In fielding a comprehensive global Culture of Cybersecurity Survey, ISACA and CMMI Institute sought to identify those organizations that have excelled at understanding the necessary cultural characteristics and organizational practices, and managing the behavior of employees tasked with defending their digital assets, networks and intellectual property—in other words, organizations that are skilled at engaging every employee in their cybersecurity mission.

"Enlisting the entire workforce to mitigate the enterprise's cyber risks is an emerging practice," says Doug Grindstaff II, SVP of Cybersecurity Solutions at CMMI Institute. "We are hearing a lot of feedback about how organizations are moving the needle on employee involvement. It's challenging, but organizations are rightly concerned by the growing sophistication of cyberattacks. And the best way to counter that is by taking an 'all-hands-on-deck' approach and aligning the organizational focus on the things that matter most."

Attributes of a Cybersecurity Culture

Fighting cybercrime is an enterprise-wide concern. That's because in today's digital workplace, a steadily growing number of essential business functions are performed online. In many organizations, across a wide range of industries, key customer data or intellectual property may be accessed by employees on an almost daily basis. Such widespread activities encompassing a workforce's shared history and familiar routines constitute part of an organization's "cyber culture."

To examine culture in the context of cybersecurity requires delving into the personal beliefs, unconscious biases, and habits that inform these security-related behaviors across the enterprise. Those findings, in addition to IT-related security measures, comprise the fabric of an organization's cybersecurity risk profile.

1) https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=1012
2) https://www.weforum.org/projects/cybercrime
3) https://hbr.org/2012/04/the-new-science-of-building-great-teams

What is an effective cybersecurity culture? The study indicates that organizations that have established an effective cybersecurity culture have employees that:

- Recognize their role in endpoint security
- Participate in regular training programs
- Actively engage with the behaviors and habits outlined by their cybersecurity program

As a result, these organizations experience benefits such as:

- Increased visibility into potential threats
- Reduced cyber incidents
- Post-attack resilience to resume operations
- Increased capacity to engage in new business
- Consumer trust in their brand offerings

However, for many organizations, building an effective cybersecurity culture remains a work in progress. Only 5 percent of organizations today believe that no gap exists between their current and desired cybersecurity culture. A full third see a significant gap. These firms have yet to experience how a strong cybersecurity culture will impact operations or create brand loyalty and a competitive advantage. While many organizations recognize that gap, they don't know which practices or programs to institute—and they generally lack a cohesive management plan.

But change is possible. Organizations that are confident in their ability to manage or transform their cybersecurity culture have outlined their best practices, providing a roadmap for those who seek to make similar progress.

"Behavioral norms across the board are essential elements of every cybersecurity program," says retired U.S. Air Force Brigadier General Greg Touhill, ISACA board director, first United States Government Federal CISO, and current president of Cyxtera Federal Group. "Doing the right things, the right way, and at the right time has become a strategic objective."

Section 1: **HALLMARKS OF A HEALTHY CYBERSECURITY CULTURE**

Nearly nine in 10 of the 4,815 respondents participating in this global study believe that establishing a stronger cybersecurity culture would increase the profitability or viability of their organization. As Touhill says, "Business is recognizing that cybersecurity is no longer a cost center, but a business enabler."

An effective cybersecurity culture enables a virtuous circle in which employees, understanding their roles and responsibilities, act as human firewalls. When cyberattacks occur, the enterprise responds in a resilient manner, either by preventing the attack or speeding up the organization's response and recovery cycle.

"Cyberattacks capture public attention through positive or negative headlines," says Grindstaff. "A quick response is critical, and best-in-class enterprises are continually building their security capabilities and resilience, and thus are in the best position to protect their public trust and enhance brand reputation."

Within the enterprise, these dynamic interactions foster communication and understanding across department or geographic siloes. Organizations can leverage this alignment on security to speed legal compliance with ever-changing regulations or strategic rollouts of new technology, adding greater adaptability to the enterprise as a whole.

These advantages are universally understood—but hard to achieve.

Several important business benefits have been achieved by the 40 percent of organizations that express strong satisfaction with their cybersecurity culture. Within that group, a resounding 84 percent of employees say they understand their role in cybersecurity enforcement and 92 percent say that their C-level executives share an excellent understanding of the underlying issues.

In organizations that have yet to establish an effective cyberculture, 58 percent cite a corresponding lack of a clear management plan or KPIs. The results suggest organizations with a weak cybersecurity culture become more vulnerable to:

- Cyber breaches
- Data loss
- Regulatory penalties
- Missed business opportunities
- Poor customer retention

"Organizations need to establish KPIs to get baseline measurements; otherwise you can't track improvements," explains Steven J. Ross, executive principle of Risk Masters International and author[4] of *Creating a Culture of Security*. "Next, you have to spell out policies for your workforce. Otherwise, generalized risk awareness will not translate into routine actions. The goal must be to foster an intentional security culture, based on habits of action."

How you both frame and present the security challenges to employees matters. According to Ross, steps that reduce or eliminate the negativity associated with risk, threat and enforcement will strengthen organization's cybersecurity culture.

"Most people do not enjoy being told what they cannot do, even if they know they should not do those things. When security is framed as trust, consistency, reliability, predictability and productivity, it becomes easier to enlist others in a culture-strengthening exercise."[5]

— Steven J. Ross

MIND THE GAP

Is there a gap between the current and desired state of your organization's desired cybersecurity culture?

- 32% Significant gap
- 63% Minor gap
- 5% No gap

Source: ISACA/CMMI's 2018 Cybersecurity Culture Study
www.isaca.org/cybersecurity-culture-study

MIXED REVIEWS FOR CYBERSECURITY CULTURE

How would you characterize the health of your organization's cybersecurity culture?

- 37% Very good
- 33% Good
- 30% Fair/Poor

Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

4) Steven J. Ross' book on ISACA website: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx
5) "Creating a Culture of Security" – pages 76 and 77

Section 2: **ESTABLISHING OWNERSHIP AND A PLAN**

Managing a successful cybersecurity culture requires a leader and a plan—yet only 58 percent of organizations have outlined a cybersecurity culture management plan or policy. The ad hoc alternative, going without a plan, poses a much more difficult challenge for those organizations seeking to obtain employee alignment with their objectives.

Accordingly, the human side of cybersecurity starts with accountability and responsibility for managing and participating in the program. One problem organizations face is determining stewardship for the program. The vast majority vest that responsibility in either their CISO (60 percent) or CIO (47 percent). And only 6 percent avail themselves of Human Resources, a potential partner that interacts with the entire workforce.

Successful communication is a two-way street—one that usually starts with listening. Yet more than half—53 percent—of organizations have not taken measures within the last year to assess their employees' views or understanding of the organization's cybersecurity culture or guidelines. Experts say that exposing or challenging these unconscious employee assumptions or biases about cybersecurity is crucial to instilling a culture of personal responsibility.

BUILDING A CYBERSECURITY TEAM WITH ORGANIZATIONAL REACH

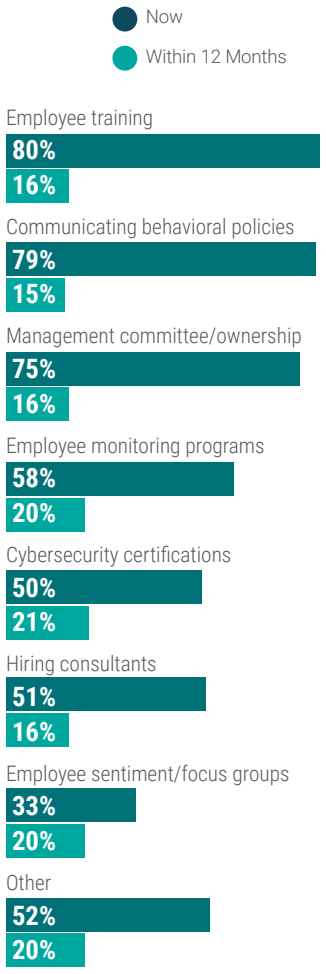
To instill greater employee buy-in across the enterprise, consider forming a cybersecurity culture team. Draw members from these cross-functional teams who can oversee the following:

- **Senior Management** sets cybersecurity as a standing agenda item at board meetings, ensures adequate resources, and addresses conflicts when security concerns and business objectives are not in alignment.
- **Information Security** educates business units on the most effective security processes.
- **IT Department** maintains technology infrastructure and up-to-date technical measures and collects data for cybersecurity analysis.
- **Human Resources** leverages its capacity for training, workshops or games with insight on staff roles, processes and behavior.
- **Legal** provides rapid feedback on international and national regulations, and aligns behavior monitoring with workplace privacy laws.
- **Marketing/Communications** provides skillset to educate staff and promote policies through in-house channels, emails, tip sheets, posters, webinars and company intranet.

Cross-functional cybersecurity teams can rapidly implement cybersecurity pilot programs or training rollouts. Such teams facilitate information sharing, analysis and the ability to course correct the next program cycle.

PLANS TO IMPROVE CYBERSECURITY CULTURE

Which steps will your organization take to improve its cybersecurity culture?



Note: Multiple responses allowed
Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

Section 3: **WINNING EMPLOYEE AND MANAGEMENT BUY-IN**

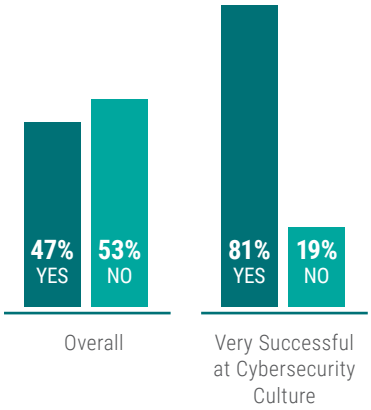
Organizations that are able to successfully manage or transform their cybersecurity culture didn't just stumble into this success. They engage in best practices and socialize their ideas. A key practice, undertaken by nearly half of these high-achieving organizations, is to annually measure and assess employee views. The results indicate that there's plenty of room for growth: 34 percent believe that their workforce clearly understands their role in achieving the organization's desired cybersecurity culture; 47 percent say that their workforce only 'somewhat' understands it; and 19 percent of respondents believe that their workforce has either a minimal or no understanding of it at all.

According to Touhill, these organizations recognize that instilling best practices is not a one-off activity but an ongoing process. "Habit patterns are essential in building a solid structure," Touhill says. "Habits are the intersection of knowledge, skill and desire."

Those surveyed agree, with 57 percent citing regular, hands-on training as more valuable than the 19 percent who cite rewards as a means to spur protection of information resources. Organizations seek to obtain employee buy-in with best practices such as group recognition (48 percent) and written performance evaluations (43 percent), outpolling options such as verbal performance evaluations, informal discussions or financial rewards.

TAKING THE PULSE OF CYBERSECURITY CULTURE

Has your organization measured or assessed employee views about its cybersecurity culture in the past 12 months?



Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

SPREADING THE WORD ON CYBERSECURITY

Cybersecurity expert Ross suggests additional best practices for communicating organizational policy:

- Outline security protocols and guidelines during each new employee's onboarding process.
- Provide additional training for current employees on a quarterly basis, upon receiving new hardware or software upgrades, or at the start of new work processes.
- Customize security training by individual awareness, technical difficulty or department risk profile. For example, financial departments work with more personal data than customer service.
- Conduct deep dives into security training via small groups with individual instruction.
- Select an ombudsman who is willing to field questions and provide feedback.
- Leverage public awareness of cyberattacks from news headlines to discuss the enterprise's security posture during company meetings.
- Establish contact points and conduct mock drills for employees to follow during an actual cyberattack.

When employees understand not only what procedures are necessary, but also why they are necessary, organizations are more successful at asking their workforce to adopt new policies or improve procedures for password management, cloud backups, device updates or new technology such as biometric scanning.

Section 4: **TAKING THE RIGHT MEASUREMENTS**

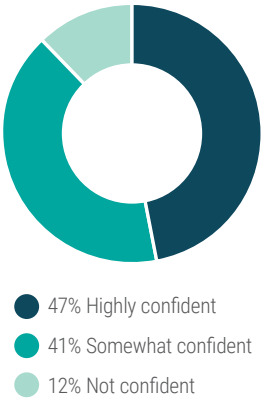
Topline business goals and baseline measurements are essential elements of any strategic plan. After all, you can't fix what you don't measure. For a cybersecurity culture plan, organizations should consider documenting employee mindset, compliance and participation in cybersecurity risk prevention and, if necessary, work toward improvement.

However, nearly a third of those organizations that have a plan in place nonetheless fail to establish goals or outline KPIs to help ensure the plan's success. Established KPIs enable organizations to benchmark a target audience's current level of understanding of any cybersecurity protocol. Organizations can also measure an employee's ability to follow guidelines in day-to-day operations or report a suspicious email, behavior or incident. This information enables training to be targeted and also points to any needed interventions.

Of course, aligning the entire workforce with the organization's cybersecurity policies requires a significant capital investment. ***Organizations that report a significant gap between their current and desired cultural state are spending 19 percent of their annual cybersecurity budget on training and other tools. In sharp contrast, those firms reporting "no gap" in their desired cybersecurity culture are spending more than twice as much, at 43 percent.*** But it's not all about money. ISACA Board Chair Rob Clyde believes that greater organizational communication is needed to discuss attempted threats and ongoing risks. Many do not share this information, fearing reputational damage. "However, individuals tend to underestimate the potential damage and overestimate technology's ability to limit such incidents," says Clyde.

MANAGING TO CHANGE THE CULTURE

How confident are you in your organization's ability to manage or transform its cybersecurity culture?



Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

Directing your cybersecurity team to share examples of successful or thwarted attacks on the organization's digital assets, cloud servers, IT security tools or log files leverages a positive aspect of group psychology and social norms. "Individuals feel more invested in the shared responsibility for their online behavior," says Clyde.

EQUIPMENT UPDATES AS TRAINING OPPORTUNITIES

CMMI's Grindstaff recommends weaving cybersecurity best practices into ongoing equipment requests and software updates by employees. Organizations can customize instructions with follow-up emails when employees:

- Update passwords or use new encryption methods
- Bring or request personal devices such as laptops, tablets, cell phones and USB thumb drives for use in the workplace
- Begin new job responsibilities that involve sharing, storing, downloading or transporting data
- Sign onto VPNs or log into unknown networks

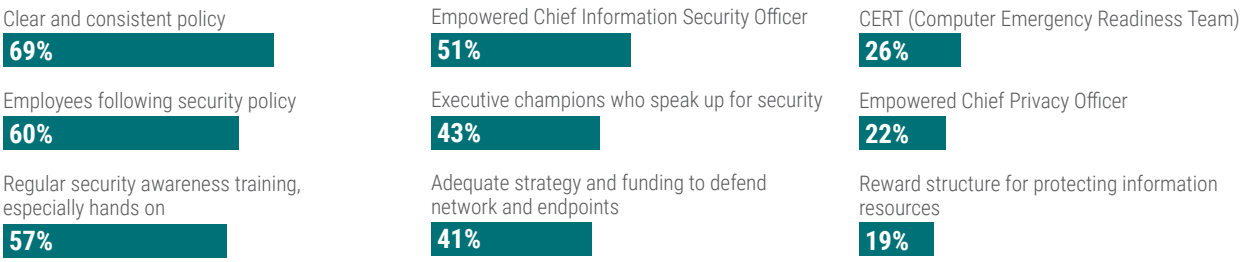
"A problem occurs when experts communicate cybersecurity practices at a highly technical level," says Grindstaff. "You need to deconstruct that information and make it accessible. You must democratize this complicated material for the entire organization."

Section 5: **TRAINING AND PRACTICES OF SUCCESSFUL ORGANIZATIONS**

New avenues for cybercrimes are multiplying, and not always because of technological advances. Often, societal norms are providing new vectors into the enterprise. Employees who are comfortable with making public disclosures on social media or using unsecured devices (BYOD) install unapproved software (also called "shadow IT") and provide additional avenues for credential theft. The risk landscape changes quickly. With so many vulnerable touchpoints, security-conscious organizations must also address human fallibility.

STRENGTHENING YOUR CYBERSECURITY CULTURE

Which steps does your organization take to strengthen its cybersecurity culture?



Note: Multiple responses allowed Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

The ISACA and CMMI survey finds that nearly four in five organizations have ramped up training centered on risk awareness, privacy policies and data protection. However, potential threats via community or social media interactions are only covered by half of the organizations.

Often, the training doesn't go far enough. For example, 83 percent of employee training programs are conducted online (computer-based training) versus through hands-on or in-person training, which is conducted by slightly fewer than half of the surveyed organizations (47 percent).

Specialized training is necessary to create a nimble and responsive workforce that can recognize and respond appropriately to new cyberattack methods. Even when individuals are aware of potential risks, they may not be equally familiar with the best response or solutions.

"Continual cybersecurity training and exercises significantly increase the capabilities of the personnel which, in turn, reduce the cyber risk of the organization," says Touhill. "Like high-performing athletes, constant improvement in cyber skills will yield championship results."

Some passive restraints are useful. Embedding compliance into the natural workflow through hardwired prompts for password updates, for example, or setting calendar commitment defaults for system updates, leverages the protection afforded by software and technology.

Some organizations go further, however. These enterprises conduct active pilot programs, tailored to a specific department's processes or access to data. Employees receive mock phishing emails or attachments that could potentially contain malicious code. Their responses are monitored for follow-up training or specific interventions when high-risk behavior is uncovered.

"At my former company, we suffered a security breach that affected 50 million users," says Heather Wilde, Chief Technology Officer, ROCeteer. "The breach was contained quickly due to the training and procedures we had in place. More importantly, the damage to the brand was minimal due to the communication we had with the customers throughout the investigation."

Organizations may find it useful to incorporate games into training workshops, with individuals playing different roles to show how a cybercrime could happen and how to prevent it. The qualities of improvisation and physical involvement in gaming are known to improve learning retention while also building shared purpose and sense of community. Personalized training workshops that include an interactive element such as Q&As provide a forum to elevate security-conscious employees with rewards such as T-shirts, hats or gift certificates.

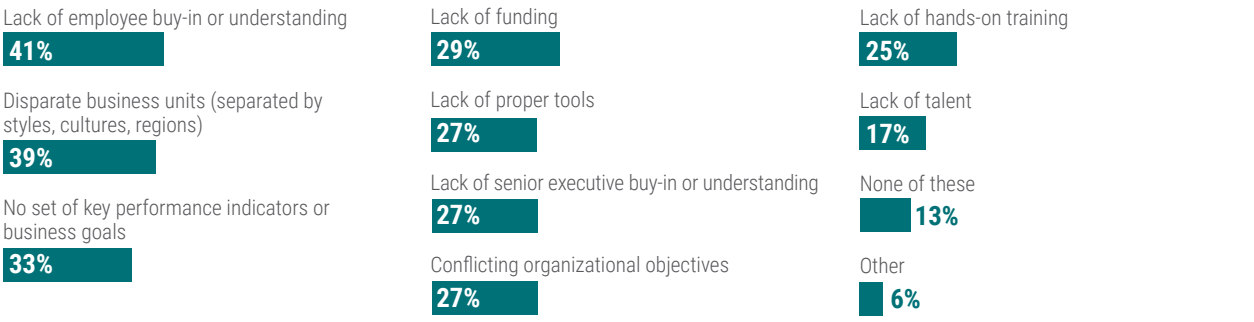
"When organizations move away from a compliance-driven, checkbox mindset to one focused on risk-based capabilities, it reorders the enterprise's focus in a Copernican shift," says Grindstaff. "In the digital age, we will never completely eradicate cybercrime. Employee training that goes beyond awareness to incorporate possible responses and instill a sense of ownership and responsibility creates organizational resilience. You bounce back, having detected and mitigated the threat."

Section 6: **THE BOARDROOM IMPERATIVE**

Cyber threats pose financial, operational, legal and market risks that can impact the enterprise's mission in real-time. Traditionally, any such threat (whether related to technology or otherwise) is the board of directors' statutory purview.

THINGS THAT INHIBIT CULTURAL IMPROVEMENTS

What factors may inhibit your organization from achieving its desired cybersecurity culture?



Note: Multiple responses allowed Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

Not surprisingly, the success of any program involving cross-functional change is greatly enhanced by the advocacy of C-suite leaders.

Among the organizations that perceive a significant gap in achieving their desired cybersecurity culture, one in three cite a lack of executive support as the major stumbling block. Other barriers to a cohesive culture include the burdens of underfunding, conflicting organizational objectives, and siloed business units separated by styles, cultures or regions.

As a result, these organizations experience business problems and competitive disadvantages such as data breaches, legal/regulatory penalties, brand mistrust, low employee engagement, and poor customer retention.

"No matter how much training you provide, and what incentives you provide your team, if they don't see leadership following the process, then everything will fall apart," says ROCeteer's Wilde. "In order to have a strong culture, you need strong leadership to model it."

Organizations with successful cybersecurity cultures tend to have C-suite executives who reinforce behavioral norms when they lead by example. They appoint—or become—a senior-level champion, participate in town hall discussions, allocate budgetary support, hire consultants, and do the research to assess the enterprise's risk and capabilities.

"It's not necessary for CEOs or board members to be technical experts on cybersecurity to advance the organization's culture on cybersecurity," says ISACA's Clyde. "What does matter is their support and buy-in."

To obtain that support, experts recommend that CISOs and CIOs translate their understanding of cybersecurity concerns into a compelling business case. They should detail how security issues will impact corporate assets, new product development, market strategy and other aspects of the enterprise's mission. As Grindstaff says, "the goal is for cybersecurity risks to get equal consideration when organizations determine their immediate and long-range priorities."

Section 7: **SIZE, INDUSTRY AND REGIONAL VARIABLES**

When viewed geographically, responses to the cybersecurity culture survey underscore the success of enterprises working to spread awareness and concern for cybersecurity threats. This is not surprising, given the diversity of global business initiatives, particularly in the cloud era. Across all seven global regions, 47 percent, or nearly half of those respondents, express confidence in their ability to manage or transform their cybersecurity culture.

By coincidence, half (57 percent) of all respondents in very large global conglomerates (with 15,000 or more employees) and small organizations (with 50 employees or less) express a high level of confidence about managing their cybersecurity culture. Perhaps managing or transforming a culture is made easier either at the extremes where individuals work closely together or where sufficient human and budgetary resources are devoted to understanding and managing a far-flung enterprise.

EXPLORING DIFFERENCES IN THE QUEST TO OBTAIN EMPLOYEE BUY-IN

How select industries, regions and organizational size impact the quest to obtain employee buy-in to cybersecurity culture.

Regional Snapshot

	Extremely/Very Successful	Somewhat Successful	Minimally/Not Successful
Africa	34%	39%	27%
Asia	39%	44%	17%
Europe	37%	51%	12%
Latin America	38%	43%	19%
Middle East	41%	41%	18%
North America	45%	44%	11%
Oceania	28%	53%	19%

Industry Snapshot

	Extremely/Very Successful	Somewhat Successful	Minimally/Not Successful
Finance/Bank	47%	42%	11%
Tech Services	48%	41%	11%
Gov/Military	31%	53%	16%

Organizational Size Snapshot

	Extremely/Very Successful	Somewhat Successful	Minimally/Not Successful
Under 1,500 employees	36%	45%	19%
Above 1,500 employees	43%	45%	12%

Note: Multiple responses allowed Source: ISACA/CMMI's 2018 Cybersecurity Culture Study

Even when the data is divided along industry lines, similar results are clustered among a wide range of business sectors. Half of all financial and banking institutions, for example, express a high level of confidence in their cybersecurity culture. In contrast, nearly two-thirds of the utility organizations and enterprises concerned with mining, construction, petroleum and agriculture identify as only somewhat satisfied with their culture.

This could indicate that some industries start their journey to greater cybersecurity with the inherited strength of a naturally collaborative, open and communicative workforce. The homogeneous results here may also signal that many organizations are still midway in their efforts to foster workforce readiness and engagement on cybersecurity issues.

"We're finding that it's very possible to move the needle on employee engagement," says ISACA board chair Clyde. "No one has to become an expert to understand how they should respond. It's a matter of aligning the best practices with the organization's mission and risk profile. Once you consider every employee potentially responsible and tailor your plans accordingly, an effective cybersecurity culture can be created and well-managed."

About the Cybersecurity Culture Study

ISACA and the CMMI Institute conducted the Cybersecurity Culture Study in June 2018. The online survey was completed by 4,815 business and technology professionals around the world, and offers insights into organizations' current and desired security cultures, and what the organizations with the strongest security cultures are doing right. For full results, expert insights and related materials, visit www.isaca.org/cybersecurity-culture-study.