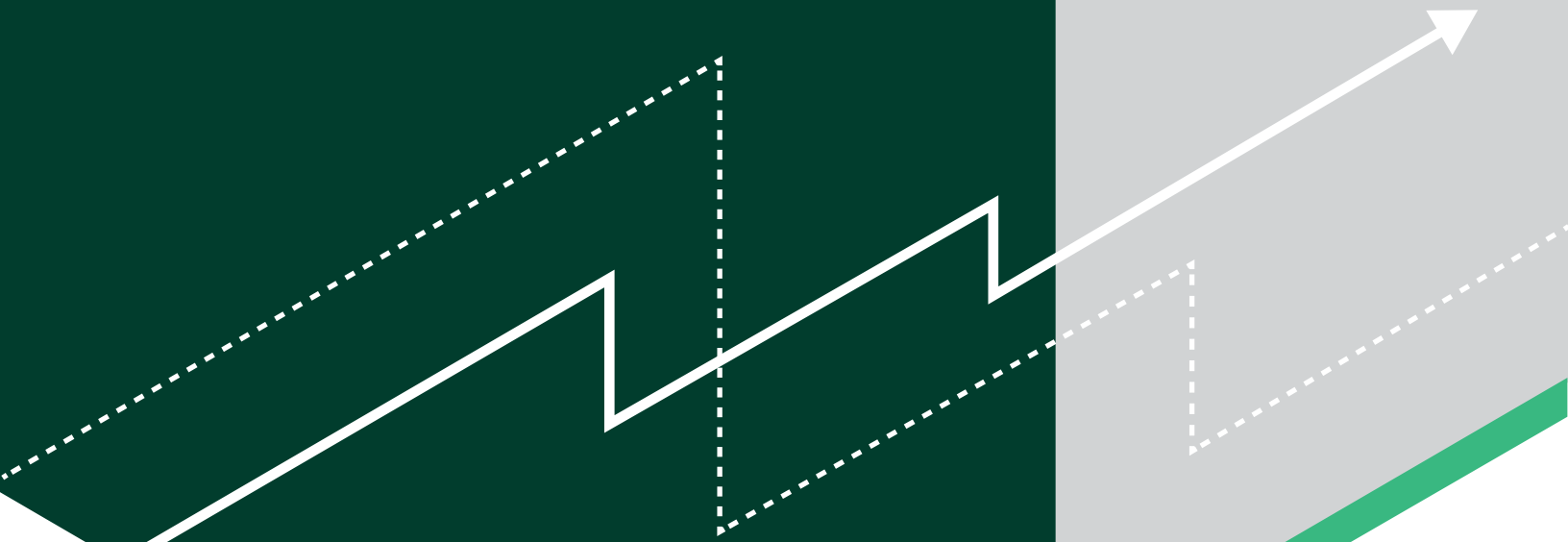
A Forrester Consulting
Thought Leadership Paper
Commissioned By KnowBe4

April 2020

The Rise Of Security Culture

Security Leaders' Journeys To Embed A Strong Security Culture Throughout Their Organizations



FORRESTER®

Table Of Contents

Project Director:
Vanessa Fabrizio,
Market Impact Consultant

Contributing Research:
Forrester's Security and Risk Research Group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

94% of respondents said security culture is important for business success.

63% of security leaders expect a strong culture to lead to increased customer trust.

Executive Summary

Security culture is a buzz-phrase whose use is proliferating throughout the business world. As overall security becomes mandatory for business success, security leaders recognize that they need a strong security culture to thrive. Most leaders believe that they have succeeded in building a strong security culture; however, they are misguided. In our recent survey of security leaders, nearly three-quarters reported that their organizations experienced a security incident in the last year, yet more than a third said their businesses still struggle to get employee buy-in and participation in security initiatives, which shows room for growth in corporate security culture. Companies need to act, as leaders universally agree that a strong security culture is necessary for business success.

In November 2019, KnowBe4 commissioned Forrester Consulting to evaluate security culture across global enterprises. Forrester conducted an online survey with 1,161 respondents who have managerial duties, or higher, in security or risk management. We found that leaders know the value of a strong security culture but are struggling to define and implement with the speed of the market.

KEY FINDINGS

- **Security culture is a business priority.** There is a common misperception that companies' motives for security initiatives are preventative. However, close to half of our respondents indicated their main motivations for building a strong security culture are business success and integrity. And almost all (94%) security leaders agree that a strong security culture is important for business success.
- **Security culture is not universally defined.** Although 94% of security leaders believe security culture is important, they have not agreed on what the term means. Our respondents were split into five different groups, all with similar, but different, definitions of security culture. In the absence of an industry standard definition of security culture, security leaders must "fake it till they make it" by defining their own measures of a strong security culture while simultaneously trying to implement one at their organizations.
- **Decision makers are overconfident in their current security cultures.** Ninety-two percent of security leaders said they have embedded security culture in their organizations; however, these same leaders are still experiencing security incidents and have yet to merge their security strategies with their overall business strategies. Further, these leaders' organizations have low employee buy-in, a critical factor in a strong security culture.
- **Strong security culture will yield high customer satisfaction.** Security leaders equate a strong security culture with customer approval. Sixty-three percent of respondents expect an increase in customer trust as a result of a strong security culture, and over half expect it to increase their brands' value.

FORRESTER®

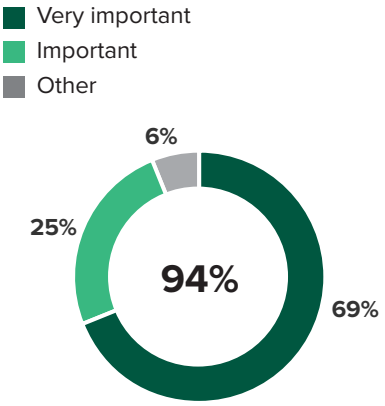
Security Culture Is A Business Priority That Leaders Are Working To Define

It's not up for debate: 94% of Forrester's respondents indicated that security culture is important to the overall success of their organizations (see Figure 1). As a result, security leaders are motivated to strengthen their security culture out of business principals, not fear. However, as leaders embark on this journey, they have not yet defined what security culture means universally.

- **Business principles are the main motivation for building a strong security culture.** Due to the increase in security breaches, it is common to think organizations are just trying to create a risk reduction mechanism when thinking about security culture. However, Forrester's data shows the opposite. Building business success (49%), business integrity (43%), and a sense of customer security (41%) were security leaders' top motivations for creating a strong security culture (see Figure 2). In comparison, a significantly smaller group of respondents said they were motivated by past security breaches (18%) or observing security breaches at other companies (23%).
- **Security culture is not universally defined.** Leaders agree security culture is pivotal to success; however, the term means different things to different people. We encountered 758 unique definitions fitting into the following five categories:
  - **Compliance with security policies (29%).** Respondents used the following sentiments to define culture: "Security culture is adherence to policies and doctrines used within the organization to minimize risk," and, "Everyone sticks to company policies regarding security whether it be using computers or other devices."
  - **Awareness and understanding of security issues (24%).** Respondents used phrases such as "a constant awareness and mindset that is analytical, focused, and open to perceive and adapt to changing situations to ensure prevention of loss or lack of oversight" and "the way staff are trained to deal with security related issues."
  - **A shared responsibility across the organization (22%).** Respondents noted: "The most important thing is everyone should understand that security is not only the responsibility of the security department, but .everyone should be responsible for security," and, "It is everyone's role and responsibility to maintain the security policy."
  - **Advocacy and support (14%).** Respondents used wording like "group of people who influence decisions about the security of an organization" to describe security culture.
  - **Security embedded in the organization (12%).** Respondents shared sentiments similar to the following: "We put security in high regard throughout the company. Our buy-in to upgrading and maintaining security is one of our top concerns."

Figure 1

"How important do you believe security culture is to your overall organization?"



Base: 1,161 global enterprise security or risk managers who influence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

FORRESTER®

While all these definitions relate, security culture is clearly still a formulating concept. Security leaders reported that culture is pivotal to success, but they could not agree on what security culture means. In some cases, respondents didn't even grasp the vastness of security culture, as their definitions were limited to compliance-based issues. The inability to accurately define such a huge initiative explains the overconfidence depicted in the next section.

Figure 2

"Which of the following would you consider a top driver of your organization's security culture initiative?"

Base: 1,161 global enterprise security or risk managers who influence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

Business benefits are the top motivations for building a strong security culture.

FORRESTER®

Leaders Are Overconfident That Security Culture Is Embedded In Their Organizations

A strong security culture will not only protect you from risk, but it will also ensure that the whole organization shares a common vision and set of values on the topic. Security leaders know that security culture is mandatory for success in today's world, and 92% believe they have successfully embedded it within their own organizations (see Figure 3). However, this overconfidence is not necessarily matched by capabilities. Forrester's study found:

- **Leaders are overconfident in their ability to prevent a data breach.** Ninety percent of respondents said they are confident in their organizations' ability to prevent a data breach; however, 72% of respondents reported that their organizations had a security incident in the last 12 months. This data suggests a disconnect between organizations' perceptions and their actual capabilities.
- **While employee buy-in is a critical component to security culture, it is lacking in many organizations.** Forrester's respondents recognized that to build a strong security culture, they need employee participation. The top measures of security culture success are (see Figure 4):
  - Employee awareness around cybersecurity responsibilities (59%).
  - Naturally adopted security behaviors and practices (58%).
  - Security policies that are being followed by the organization (57%).

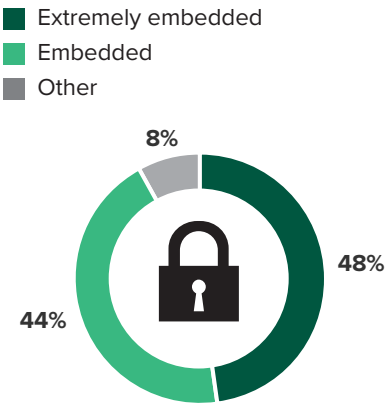
  However, employee buy-in is the biggest challenge organizations face when attempting to build a stronger security culture. Respondents identified a lack of understanding around security issues as their top challenge in creating a strong security culture (39%). Further, organizations struggle to shift negative attitudes around security culture; 39% of leaders reported that their employees believe security impedes on their productivity, and 36% believe that their employees do not see security as their responsibility (see Figure 4).
- **Security is still seen as an IT issue, not a business initiative.** Organizations see security as a business necessity but are not giving it the business's attention. Security leaders are more likely to discuss security with tech leaders than any other stakeholder. In fact, 26% of respondents indicated they connect daily with IT leaders on the topic of security. Only 19% of the respondents said the same about their business unit leaders, and only 15% said the same about their executives.

  Perhaps more concerning, 31% of leaders reported that their organizations still have informal relationships between their security initiatives and corporate business functions. If companies want to make a real security impact, this has to change.

72% of leaders said their organizations had a security incident in the last 12 months.

Figure 3

"To what extent do you feel security culture is currently embedded in your organization?"



Base: 1,161 global enterprise security or risk managers who influence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

FORRESTER®

Figure 4

Base: 1,161 global enterprise security or risk managers who influence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

Security Leaders Anticipate A Better Security Culture Will Enable The Business And Create Customer Trust

Security leaders recognize that their organizations need a strong security culture for overall business success, but more specifically, leaders believe that a robust security culture will create customer trust, increased brand value, and business support. Our research shows that firms with a strong security culture in place predict strong business benefits:

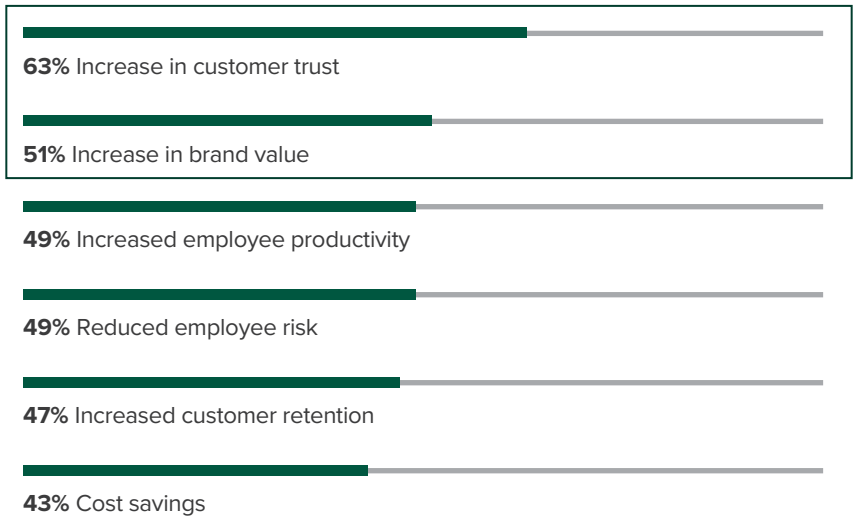
- **Security leaders expect strong culture to create stronger customer trust.** When a company successfully builds a strong security culture, its customers take notice. Sixty-three percent of respondents expect an increase in customer trust as a result of a strong security culture (see Figure 5). Further, over half of respondents predicted a strong security culture would increase their brands' value.
- **Strong security culture leads to employee and business support.** As a result of implementing a strong security culture, 44% of respondents anticipate employee knowledge around cybersecurity responsibilities would increase, and 41% expect more employee compliance with security policies. These internal improvements bring about external business benefits for these organizations.

44% of respondents anticipate increased employee knowledge around cybersecurity responsibilities as a result of a strong security culture.

FORRESTER®

Figure 5

"What external business benefits do you anticipate if your company successfully builds a good security culture?"
(Select all that apply.)



Base: 1,161 global enterprise security or risk managers that influence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

Organizations expect a strong security culture to lead to increased customer trust, customer retention, and brand value.

Key Recommendations

Forrester's in-depth survey of global security leaders showed that organizations understand that a strong security culture yields more than just compliance and avoidance of breaches. They know that a strong security culture brings benefits like increased customer trust and integrity and is essential to a successful business. To achieve these results, security leaders should follow these important recommendations:

Define and measure your organization's security culture. Security culture represents the vision, values, ideas, customs, and social behaviors of an organization, which ultimately influence its security posture. You need to assess the level of your security culture among different dimensions to gain insight into areas such as security leadership, employee perception, and communications. There is no single ideal security culture. Determine where you would like your culture to be, and define your roadmap to achieve it.

Embed security up, across, and down your organization. For your security program to be successful, you will need many things from many different stakeholders across the organization. For example, you will need the advocacy from your board and executive management to help fund your security program and increase your visibility and influence from the organization; buy-in from the lines of business to get security project support; and awareness and proper behaviors of employees to build your human firewall. Create your security marketing and communication plan to identify exactly who your stakeholders are and what you need from them, and work with them to determine how you will build that support and change important behaviors.

Build relationships with relevant business functions — not just IT. As a key business liability, cybersecurity risk cannot be the sole responsibility of IT or security. Companies need to create an environment where there is formal and ongoing collaboration with a range of business functions, not only IT, focusing on improving both security and business performance. Do this by: 1) creating and documenting relationships between security and business (for example, an organizationwide security committee); 2) defining the objectives for the relationship; 3) collaborating with those functions on joint initiatives; and 4) determining both security and business performance success metrics.

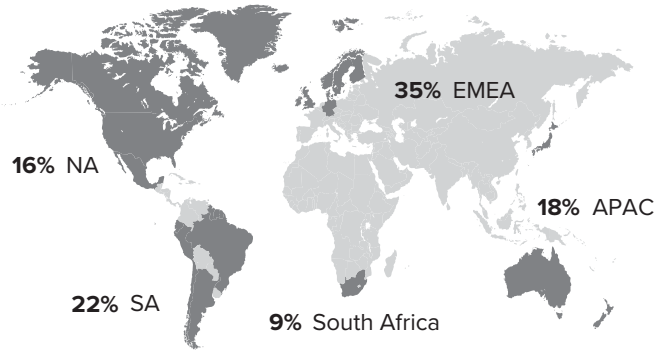
Make embedding a culture your No. 1 job. Amid today's complex security landscape, CISOs are running significant initiatives including cloud migration; Zero Trust architecture; technology upgrades; and insider threat, digital identity, and security awareness programs. Far from being purely technology programs, these initiatives require a fair dose of people, process, oversight, and technology knowledge. As you seek to have your security program adapt to the new normal, you must ensure that it is an embedded and holistic function, and you cannot be the only one doing it. You will need everyone on the journey, and this is a culture program. Make the decision to become a culture change leader; your personal courage, change, and communication attributes will be more crucial than ever.

Appendix A: Methodology

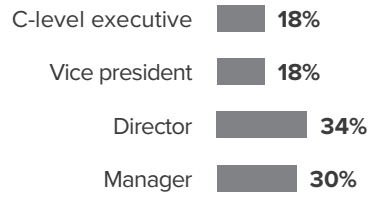
In this study, Forrester interviewed 1,161 security leaders at global enterprises in the US, Canada, the UK, Germany, Australia, New Zealand, Japan, Brazil, Mexico, Chile, Argentina, Peru, South Africa, and the Benelux, Nordic regions to evaluate their current security culture initiatives. Survey participants included decision makers in IT, security, or risk. Respondents were offered a small monetary reward as a thank you for time spent on the survey. The study began in November 2019 and was completed in December 2019.

Appendix B: Demographics/Data

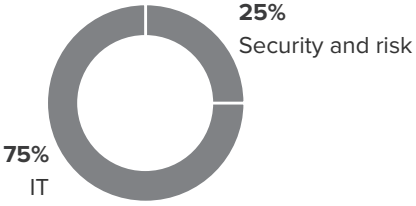
GEOGRAPHY



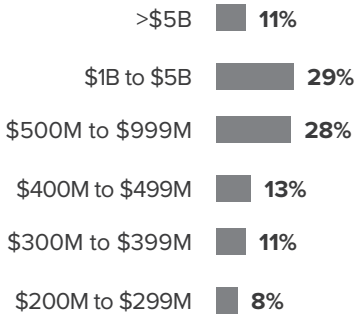
RESPONDENT LEVEL



DEPARTMENT



COMPANY REVENUE



Base: 1,161 global enterprise security or risk managers that infuence their organizations' security policies
Source: A commissioned study conducted by Forrester Consulting on behalf of KnowBe4, December 2019

FORRESTER®