KnowBe4
Human error. Conquered.

GLOBALCTI
GLOBAL SOLUTIONS. WORLD CLASS SERVICE.

The Security Culture How-to Guide

Seven Steps To Improve Your Organization's Security Culture

The Security Culture How-to Guide

Table of Contents

INTRODUCTION

The phrase "security culture" is being used a lot more often within organizations, during conversations with other security professionals and even in the media. But there is a problem: the definition is not necessarily clear, and the steps to start working toward creating a positive security culture are even less clear. Organizations only have a vague idea what that really looks like or how to accomplish it.

This guide exists to provide a high-level look at what security culture is and what actions you can take to begin favorably changing the security culture within your organization. The goal of this guide is not to give a detailed deep dive into all things security culture (though we'll provide resources for that in the future); instead it is to help readers understand the fundamentals of what security culture is and what steps you can take to move the culture needle in your organization.

It is important to understand that making a meaningful culture shift is not something that happens overnight. Dedication and consistency will lead you to great results. The more established your security culture is, the easier it is to maintain, and new employees tend to align with this culture rather quickly.

We are social creatures. Many behaviors are caught rather than taught. When we start a new job, we subconsciously adopt many of the behaviors we see. If people lock their workstations every time they walk away from their computers, new employees often pick up habits like this without giving it much thought at all because it has been socially modeled as just the way things are done here. This is the beauty of a strong and present security culture; once momentum is gained, it becomes easier to maintain.

DEFINITIONS

Defining security culture is surprisingly difficult for many organizations. Without a firm understanding of what security culture is and an idea of where you want to take your organization on this journey, failure to make meaningful and lasting change is almost inevitable. At KnowBe4, we define security culture as:

> "The ideas, customs, and social behaviors of a group that influence its security."

When defined like this, the idea of security culture seems a bit less confusing. When culture is thought of in a broader sense, not just from a security standpoint, it is often thought of as, "What people do, when other people are not watching." Although that statement is often attributed to the terms "integrity" or "character" when speaking of a single person, it also works to describe "culture" from a group perspective.

Keep this simple definition in mind when working toward changing your organization's security culture. Print it out and tape it to your monitor or write it down and put it somewhere that is visible. This can help you remember your goal and keep focused.

Introduction to the Seven Dimensions of Security Culture

In the 2019 research paper published by KnowBe4 Research called "The Seven Dimensions of Security Culture," the authors identify seven dimensions of security culture and explain how they are used to measure an organization's security culture. The seven dimensions are:

- Employee **attitudes** to security and policies
- **Behaviors**
- **Cognitive processes** surrounding security
- Quality of **communication**
- **Compliance** to security policies
- Organizational unwritten rules or **norms**
- Individual **responsibilities**

While we recommend reading more about the details of these dimensions and how they are used to measure security culture, for now being aware of them is a good starting point.

When beginning to make improvements to the organizational security culture, choosing behaviors that span a dimension or two to work on will help focus your efforts. Choosing behaviors across too many dimensions can result in slower changes compared to a more focused approach. Please note that these dimensions do not stand alone, and that improvements in one area will often influence other dimensions.

The ABCs of Culture Change

A critical concept when considering how to change a security culture, is the ABCs principle. ABC is an acronym that stands for:

- Awareness
- Behavior
- Culture

> *Awareness can influence behavior, and changing behavior can lead to a change in culture. It is a logical progression and important to remember when planning your strategy for culture improvement.*

The principle is simple, yet important. Awareness can influence behavior, and changing behavior can lead to a change in culture. It is a logical progression and important to remember when planning your strategy for culture improvement. While awareness does not automatically equate to behavior changes, it can be a powerful tool to influence it if it is made relatable. Likewise, changing a single person's behavior does not equate to a change in culture, however, changing the group's behavior does.

GETTING STARTED

Now that we have covered the essential ideas and definitions of security culture, we can discuss how to make changes. Getting started on this journey is often the toughest part. Many of the individuals tasked with improving security culture are not formally trained on how to change human behavior. Do not be discouraged or intimidated.

Here are the seven basic steps in the cycle of improvement. We will discuss each in more detail in the next few pages.

Step 1 – Choose One or Two Behaviors You Would Like to Change

Step 2 – Design a Plan to Influence Behaviors on an Organizational Scale

Step 3 – Get Leadership Buy-in

Step 4 – Communicate

Step 5 – Execute the Plan

Step 6 – Measure Results

Step 7 – Determine the Move Forward Strategy

Step 1 – Choose One or Two Behaviors You Would Like to Change

Understanding the risks your organization faces is a consideration when choosing the behavior(s) you want to concentrate on. Identifying which dimensions these fall under can help ensure that you do not spread yourself too thin. The behaviors you choose to address should align with the top organizational risk. Remember that risk is often calculated in the formula: Risk = Likelihood × Impact, so the risk you are addressing and behavior you are modifying may not be the most common, but instead may be the most impactful. Choosing the behavior(s) and dimensions to address depends on your organizational threat model and risk appetite. Referencing recent annual reports, such as the Verizon Data Breach Investigations Report (DBIR), may also provide insights into current threats which you may want to address.

Be careful not to attempt to change too many things at once and to give ample time for the change.

Is wire transfer fraud a major threat? Is ransomware your key risk? Are physical threats increasingly problematic? Knowing this can set the direction of your program. Be careful not to attempt to change too many things at once and to give ample time for the change. A good starting point would be to choose behaviors that span one or two of the dimensions to focus on and give yourself three to six months to make the changes. Once you have run through a cycle or two, you may be able to adjust the cadence based on your organization’s adoption of changes. The important thing is to not try to change too much, too fast, especially in the beginning by being too ambitious.

A Security Culture Survey will help identify the dimensions that need the most improvement and may also help you decide which behaviors to focus on. Remember that changes in one dimension can impact others. For example, if employees ignore security policies due to having a bad attitude, this could increase the risk of a ransomware infection due to non-compliance with important security controls. By focusing on improving their attitudes toward the policies, perhaps by educating them on how they impact the safety of their own information, you would likely improve compliance with the policies. This would impact two of the dimensions with a single focus on just one and reduce the risk of a ransomware infection. This is just an example, but it illustrates how these interconnect.

While executive buy-in comes in Step Three, this is a good time to stress the importance of focusing on security culture to your direct leadership. Details can follow, but just making them aware can give you a feel for their support and an opportunity to plant the seeds that will pay off later when you need resources.

Step 2 – Design a Plan to Influence Behaviors on an Organizational Scale

Behaviors can be directly influenced through formal means, like in the case of a policy creation or change, or can be done informally and socially, often through an organized effort to demonstrate the desired behavior by leadership.

For example, if an organization has historically propped open the back door for people to take cigarette breaks outside, a policy might be written or updated that specifically states that the practice is no longer acceptable. Or in a more informal way, if members of leadership that smoke start closing the door behind them, socializing the dangers of an open door, then walking to another entrance or using a badge to re-enter, others are likely to catch on to the practice and follow suit even without a formal policy change. Each method has advantages and disadvantages, however both shape the behavior of other employees.

Any additional momentum you can gain from working with others will help make the changes come faster and with less effort.

Taking on behavior change in people may feel daunting at first, especially if you tend to work in a highly technical role. Treating this like a planned technology rollout may help. Consider the dependencies of making the changes and the time it may take to get anything missing in place. Think about possible points of failure and how risks can be mitigated, etc. For those in a less technical role, applying the project management principles that work well for you in other areas will apply here as well.

When planning, ensure to identify people who can help influence these changes, even if they are not in your own department. Many of us already know at least some naturally security conscious employees across the organization. These people can be immensely effective when executing your plan on a large scale by demonstrating and advocating for the desired behaviors to others within their sphere of influence. Include them in your plan. Any additional momentum you can gain from working with others will help make the changes come faster and with less effort.

Remember that most people are social beings, and our actions tend to align with others, even if we do not realize it. Look at it like installing champions across the business who can help drive the overall messaging. If you are a global company, they can also adapt the messaging with cultural differences in mind. These individuals are an essential part of the overall success of a program because you/your team cannot be everywhere, and you will need security-minded people in all areas of your business who will be ready to assist.

Step 3 – Get Leadership Buy-in

Now that you have a plan in place, you want to get executive leadership onboard. Prepare an executive summary for them that is light on the details but heavy on why the changes need to happen, the risk to the organization if the changes do not occur, who will be involved in the plan, the resources you will need, and the intended timeline.

If possible, get a commitment from leadership to adopt and display the behavior changes to the rest of the organization.

Most executives do not want the fine details at this point, however, be prepared to provide whatever level of information they need to make their decision. If possible, get a commitment from leadership to adopt and display the behavior changes to the rest of the organization. This is where starting off with small changes can be very helpful. For example, asking leadership to ensure they lock their computer when stepping away is an easy thing to commit to and starts setting a visible example. As you progress through several cycles of change, committing to these better behaviors becomes easier for them to commit to, especially if previous changes have been relatively low friction and proven to be effective.

When speaking to the executive, you might consider approaching it like this:

> *"One of the biggest threats in our industry right now is ransomware. Because the average ransom payout is $570,000 and because the recovery costs are much higher than even that, I would like to focus on getting people to better be able to spot and report phishing emails, a top way they start the infection, to the security team so we can work on defending against them. Your commitment to mention this at a future all-hands meeting would be greatly appreciated. I can give you details later. Thanks for your support."*

This is simple, light on details and short enough to pitch in the elevator. It does not require an unreasonable commitment on the executive's behalf, but does support the action. Of course, this type of communication will vary between organizations and executives, and you may need multiple managers and executives, especially ones you report to, to commit, but it illustrates one approach. Employees look to executives to demonstrate expected behaviors and attitudes. Find ways to also promote embraced activities at the top and ensure that employees see that everyone across the business is being held accountable in driving a more security-aware culture.

Step 4 – Communicate

Step Four is all about communicating the "why" to the people whose behavior we are looking to change. This is more important than it may initially seem because we are often asking people to take additional steps to accomplish the same thing they have in the past.

Consider the example of locking a computer when you step away, even for a few minutes. While locking the computer is usually trivial, it also requires that you unlock it when you return. Where normally the person simply would get up, go to the break room and grab a coffee, now we are asking them to lock it when they leave, and most likely type in their password to unlock it when they return. That can add up to quite a few more times entering passwords throughout a normal workday. If people do not understand the reason for doing it, and it does not relate to them, it may cause friction.

This is why communication plays a key part in the success of modifying behaviors and improving security culture. It might be beneficial to inform people of the upcoming changes by sending an email to employees with a message like this. Or – better yet – get an executive to send it!

> *Our <insert team name> has discovered that there is a rise in cybercriminals who are socially engineering their way into buildings like ours, dressed as janitors, maintenance people, or even job applicants, and looking for unlocked computers to install viruses on. It only takes a moment for them to do this, and the results can include stealing employee data and identity theft among other things.*
>
> *To help counter this and to keep your information and that of your coworkers safe, we are implementing a policy where, when you step away from your computer (even for just a minute), you must lock it. Please help us keep everyone safe.*

A key secret to improving a security culture is to remove friction from the processes, this includes the tone we set when we communicate.

This is just an example to illustrate how a change like this can be communicated by showing them how the change is personally relevant. In some situations, more formal and direct communication might be more appropriate. It is important to note that a key secret to improving a security culture is to remove friction from the processes, this includes the tone we set when we communicate. We are typically better off when people see the security team as a resource or an ally rather than being seen as the opposition.

Remember the champions mentioned in Step Two? This is a great place to engage them. Champions have closer connections to the desired audience, and often, more in common with them. They can take messaging and communicate it in a way that easily relates and makes sense. It is also not “someone at HQ” asking them to do something else, but rather a peer, or someone they are more familiar with, reinforcing something that even they are doing. This is where their ability to influence and make the messaging relevant is important.

Additionally, work with other departments across the organization to reinforce the messaging in their respective communications. For example, partner with marketing to add tips/techniques to their communications or with the digital team to run banner ads on the company intranet site. Since people receive information in a variety of ways, the higher the frequency of visibility, the better positioned you are for the messaging to be consumed.

Step 5 – Execute the Plan

Your plan should have a clear goal with a well-defined picture of what success looks like. Deadlines and the times to communicate and implement each part of the plan should already be thought out. Some flexibility in the plan is to be expected, but keep an eye on the goal and measure progress, when possible, along the way.

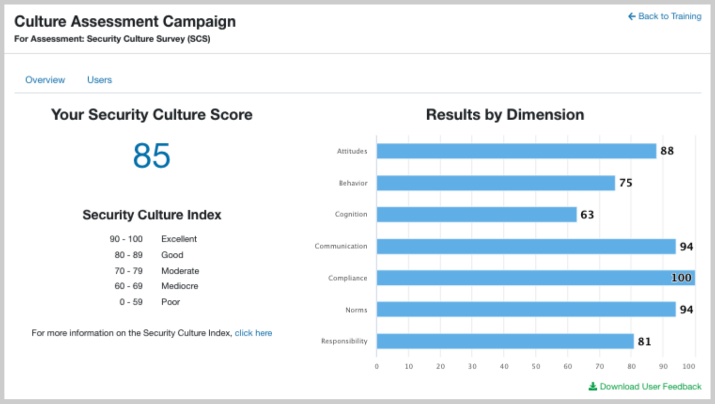
Just before you implement the plan, it is generally a good idea to get a measurement of where you currently stand by performing another Security Culture Survey, which will illustrate where you stand across the seven dimensions so you have a baseline to compare the improvements against.

Make sure to remember to involve any people you have identified as your advocates throughout the organization and be sure to also communicate with them about ways they can help and where they can go to get questions answered, separately from the larger group.

Be ready to experience some people pushing back against changes; we are creatures of habit after all. Do not take it personally. Work toward resolution wherever possible. There may be times when you discover that a part of the plan really impacts the workforce in a negative way. Keep an eye open for those types of issues, adjust and keep them in mind when planning the next cycle. Also, ensure to leverage communication as a way to promote plan progress and successes along the way. Find ways to highlight those things that are going well and the people who are driving those positive changes.

Step 6 – Measure Results

When the plan is fully executed, performing another Security Culture Survey will illustrate where you have made progress and areas where more progress might be needed. Use this information to find the approaches that work within your specific organization so you can implement them in future cycles. Note where the behavior changes in one dimension impact others so you can better understand the relationships for future planning.



Culture Assessment Campaign
For Assessment: Security Culture Survey (SCS)

Your Security Culture Score

85

Security Culture Index

90 - 100	Excellent
80 - 89	Good
70 - 79	Moderate
60 - 69	Mediocre
0 - 59	Poor

For more information on the Security Culture Index, click here

Results by Dimension

Remember to document the results in a report that can be shared with leadership. This result may not need a lot of detail, but can reinforce the improvements and make future commitments from executives and management a lot easier. Be sure to include the before and after results and any discernible changes that happened as a result. For example, something like this:

> *"Our <insert team name> just finished our latest culture improvement cycle and have found that employees showed a 20% improvement in their attitude toward security policies, which resulted in a 15% improvement in them following policies. In addition, help desk tickets related to virus cleanup dropped by 20% and the reporting of phishing emails is up 32%. This really helps us see what is targeting us so we can better prepare defenses. We look forward to our next culture improvement cycle, which we will discuss with you in the near future."*

Again, this is just one example of communication. How you communicate the results to leadership will depend on your organization and the executives you are communicating with.

Also, consider how you package the data. Providing the results by department or C-level executive may also highlight areas within the organization that need to apply more rigor and may create necessary urgency. No one wants to look bad in front of the boss, and in this case, no one department/executive wants to be the focus of potential security vulnerabilities.

Step 7 – Determine the Move Forward Strategy

Once you have met the timeline allotted for the plan or have met the goals outlined in the plan, you can review your threats and determine if you should continue to focus on the same goals or work toward others in the next cycle.

Review what worked well and what did not, adjusting your future goals to improve the odds of success. Having run through a cycle, this would be a good time to reach out to the people you identified as advocates and get their feedback and suggestions for possible future behaviors to work on. They can be an invaluable source of information that you might not hear from within their departments.

If you decide to turn your focus, remember to continue reinforcing the behaviors you have been working on so they do not fall to the side. One thing alone will not make a difference, it is the continued combination and alignment that favorably moves the needle.

THE BOTTOM LINE

Improving security culture may seem complex, especially in the beginning. However, understanding that change happens over time and is the result of positive behavior changes and habit formation, can simplify the task. Be deliberate in your actions and do not try to change too much too quickly. Communication can make a big difference in the swiftness and degree to which the behaviors change, especially if the communications help people understand why they should care about security.

Additionally, though we have been focused primarily on the professional environment, everything learned in security awareness and culture is 100% transferable to your personal life. Take the learnings home with you to your friends, family and loved ones in order to increase their security hygiene.

Future writings will go deeper into the seven dimensions we briefly covered here and will offer more technical information that may be useful as your security culture improvement program matures, however, this document and the following checklist should be enough to help you get started. The sooner you start, the sooner you will start seeing results.

Security Culture Improvement Checklist

Step 1: Choose One or Two Behaviors You Would Like to Change

□ Choose one or two behaviors to change based on risk

□ Perform Security Culture Survey to establish a baseline

Step 2: Design a Plan to Influence Behaviors on an Organizational Scale

□ Calculate timing and duration of this cycle

□ Identify ambassadors/champions within the organization

Step 3: Get Leadership Buy-in

□ Create a high-level description suitable for executives to review and commit to

□ Get leadership to commit to an action

Step 4: Communicate

□ Develop a communication plan for employees with a focus on making it relevant and partner with other departments to increase message visibility

□ Offer help and assistance to those who need it, or have concerns

Step 5: Execute the Plan

□ Have a clear goal with a well-defined picture of what success looks like and a timeline

□ Communicate with the champions and executives and offer support

Step 6: Measure Results

□ Perform another Security Culture Survey and compare

□ Create a report outlining results for leadership

Step 7: Determine the Move Forward Strategy and Repeat

□ Reach out to advocates for feedback and form ideas for the next cycle

□ Review threats and determine behavior goals for the next cycle

GLOBALCTI
GLOBAL SOLUTIONS. WORLD CLASS SERVICE.

To get started contact us today!
800-366-1711 or Sales@gcti.com

www.GCTI.com