



Introducing the Security Culture Maturity Model

KnowBe4
Human error. Conquered.

Executive Summary

Security Culture:

the ideas, customs,
and social behaviors
of a group that
influence its security.

With 85% of data breaches being caused by social engineering or human error¹, it is clear that organizations can't afford to neglect the importance of the human side of cybersecurity. Employees have become the de facto attack vector of choice for cybercriminals. Their knowledge, beliefs, values and behaviors will be the difference between protection and breach. That's why focusing on security culture is so important.

KnowBe4 Research has developed a data-driven and evidence-based Security Culture Maturity Model. The model is fueled by KnowBe4's massive security awareness, behavior, and culture dataset. This dataset is ultimately comprised of individual datapoints that we call Culture Maturity Indicators (CMIs). The aggregation of several CMIs gives the Security Culture Maturity Model unparalleled insight into the true maturity of an organization's security culture.

¹ <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>



Introduction

“Security Culture” is a hot topic. The phrase seems to be appearing with increasing frequency in online articles, security presentations, and vendor pitches. But there is a problem: the phrase is often used in ways that are absent of any real meaning.

As a result, the phrase security culture is often thought of as the same thing as security awareness and training. Those who use the phrase often do so in ways that would insinuate that security culture is something as simple as the output of security awareness and training activities. But, while security awareness and training efforts do contribute to security culture, awareness and culture are not the same. Security culture is a much richer and more intricate topic. Security culture encompasses everything related to the ideas, customs, and social behaviors of an organization and how those factors influence the organization’s security.

Defining Security Culture

One of the main reasons for all of the confusion around the phrase security culture is related to a very fundamental issue. People use the phrase without defining what it means. That leaves everything up to interpretation and assumption. As such, one goal of this body of work is to change that.

Security Culture is defined as the ideas, customs, and social behaviors of a group that influence its security.

Why is Security Culture So Important?

If there is one good thing that comes from all the media reporting about cyberbreaches around the world, it is that virtually every organization now recognizes the need to shore up their cyber defenses. Organizations are extremely interested in ensuring their long-term resilience and sustainability.

There are aspects of that story that are technology-centric, but there are also many, many aspects that are people-centric. When leaders hyper focus on the technology side of the story, they risk forgetting that technology is only part of the equation. And they risk forgetting that humans are at the center of everything.

The Cost of Not Focusing on Security Culture

With 85% of data breaches being caused by social engineering or human error², it is clear that organizations can't afford to neglect the importance of the human side of cybersecurity. Over the past few years, there has been a meteoric rise in attacks seeking to bypass technology by targeting humans. And it's working. Ransomware continues to make headlines due to large scale attacks like those that targeted Colonial Pipeline³, JBS Foods⁴, and Kaseya⁵.

This trend only grows as technology-based defenses improve. Attackers are drawn to the path of least resistance. They want to save time, effort, and cost. And because technology-based defenses can be difficult to penetrate using technology-only attack methods, cybercriminals view employees as the most attractive attack vector. Because of this, employees have become the de facto attack vector of choice for cybercriminals. Their knowledge, beliefs, values, and behaviors will be the difference between protection and breach. That's why focusing on security culture is so important. An organization's employees are at the center of everything; they can either be easy prey, or they can become an effective human layer of defense.



KnowBe4's Security Culture Expertise

KnowBe4 has more security culture experts and has invested more in the study of security culture than any other vendor. For example, KnowBe4 employees Kai Roer, Perry Carpenter, and Joanna Huisman are three of the world's most well-known and respected security culture experts. While at Gartner, Perry and Joanna headed up Gartner's research efforts into security awareness, behavior management, and culture. As part of that, they worked with thousands of CISOs and security awareness leaders around the world, advised dozens of vendors, and spent hundreds of hours reading and authoring research into these topics.

In 2019, KnowBe4 acquired CLTRe (pronounced 'culture'), a company founded by Kai Roer. Kai and his team have been providing consulting services, studying, and creating tools and processes to measure security culture for over a decade. During that time, Kai's Security Culture Framework and Security Culture Survey have been adopted and actively used by organizations of all types around the world. These tools have even been utilized and promoted by multiple governments and governmental institutions.

Both Perry and Kai are award-winning authors on the topic of security culture. Perry's book, "Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors" (2019) was recently inducted into the Cybersecurity Canon Hall of Fame, and Kai's book, "Build A Security Culture" (2015) has long been thought of as the go-to resource for security professionals looking to gain greater control of their organization's security culture.

² <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>

³ <https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html>

⁴ <https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/>

⁵ <https://www.csoonline.com/article/3626703/the-kaseya-ransomware-attack-a-timeline.html>

It's All About the Data

One of KnowBe4's core missions is to provide customers with forward thinking tools and resources needed to understand their workforce's current risks and strengths. For example, KnowBe4's platform provides reporting that allows customers to view their organizations' phish-prone percentage™, understand industry benchmarks, view risk scores, survey employees, and more.

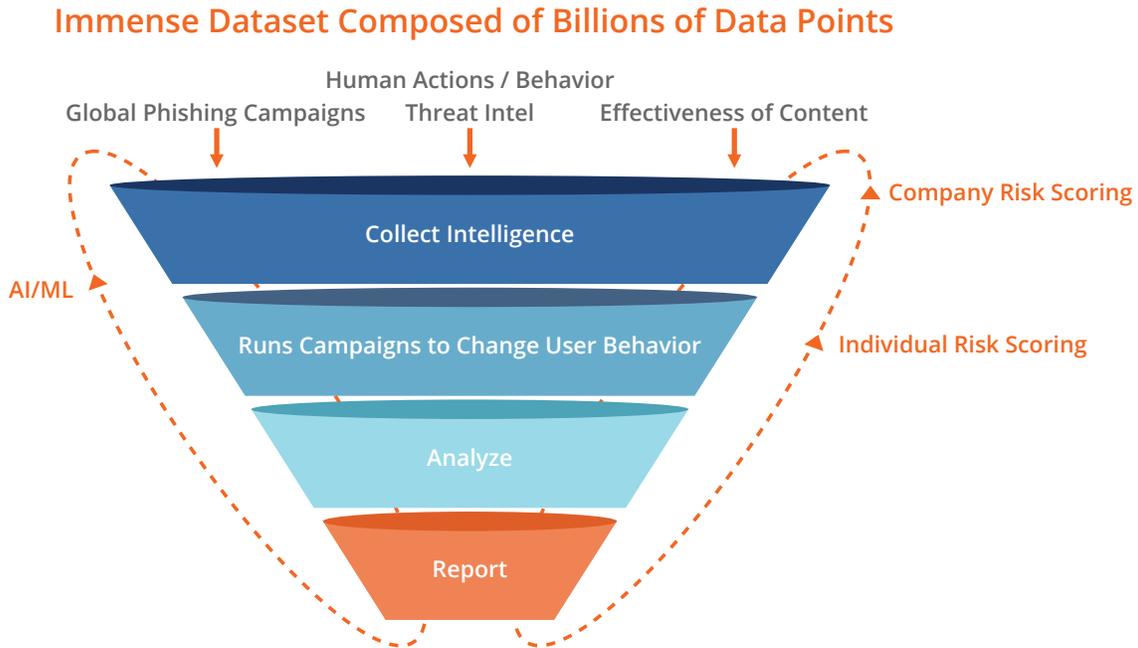


Figure 1: KnowBe4's immense dataset delivers unique value to inform our model

One side effect of being the world's most popular security awareness training and simulated phishing platform is that KnowBe4 has collected billions of data points from training campaigns, phishing simulations, and employee surveys. As a result, KnowBe4 has the largest dataset in the world when it comes to security culture.

That data is about to be used in a new and groundbreaking way: to provide the industry's first data-driven maturity model specifically geared to measure security culture.

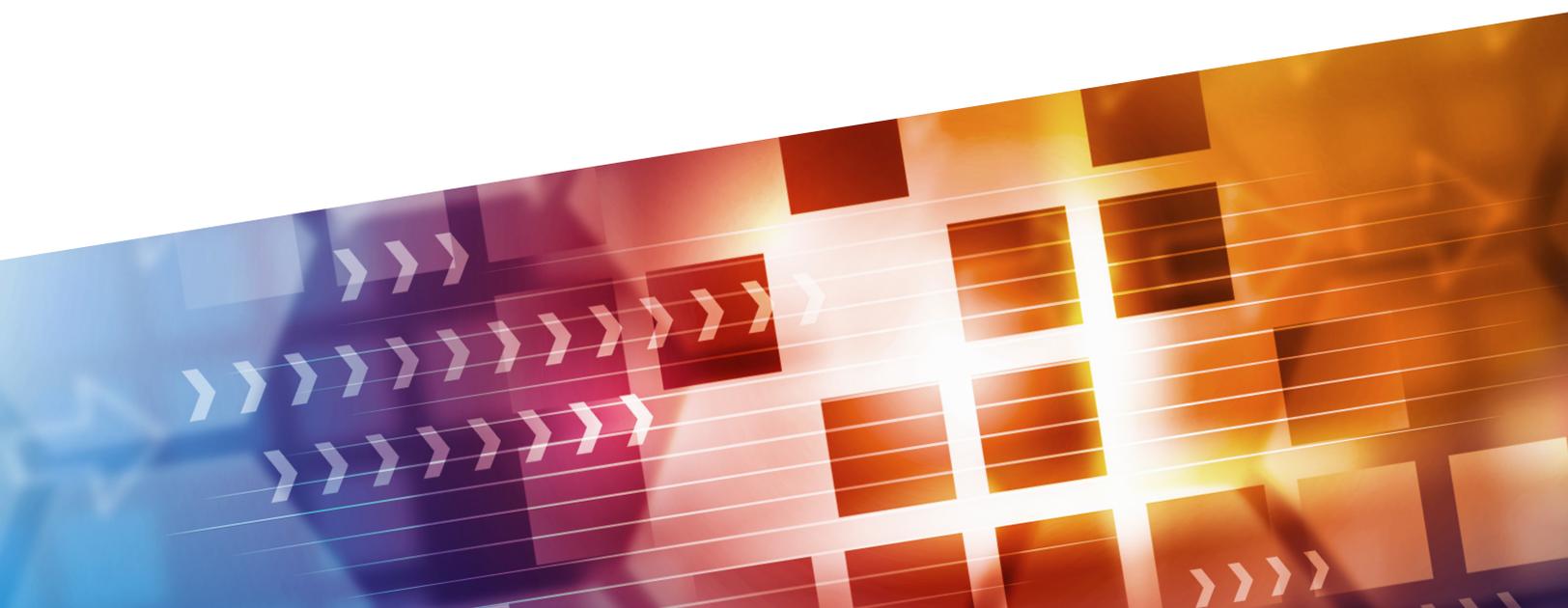
Culture Maturity Indicators

The KnowBe4 dataset is comprised of several different elements. These range from training data elements, to simulated phishing resilience data, to organizational demographics, and more. We call each of these datapoints, Culture Maturity Indicators (CMIs).

Here are a few examples of CMIs across various categories:

Security Awareness Training	Phishing & Simulated Phishing Testing	Behaviorial Data Awareness	Organizational Tone and Activities	Survey Data	Other Measurement Data
<ul style="list-style-type: none"> • Frequency of training campaigns • Delivery types (in person, online, mobile, etc.) • Content types used • Learning modules taken • Measured areas of strength or weakness • Customization/ personalization for the organization and their unique risks • Customization/ personalization for the individual based on role/department 	<ul style="list-style-type: none"> • Opened • Clicked • Attachment open • Data entered on a landing page • Exploited: user clicked on an Exploit enabled test • Macro enabled: macro on an attachment was enabled • Replied • Reported • Accuracy of reporting • Organizational patterns of use for phishing simulations (e.g. customization of templates, gamification, etc.) 	<ul style="list-style-type: none"> • Tracking & Reporting of simulated or real-world user behavior alerts • Documented policies for user behavior failures (stick) or high performance in testing/ self-reporting (carrot) • Technology/ Integration into real-world behavior alerts • Gamification 	<ul style="list-style-type: none"> • Company-wide communications regarding security policies • Executive led discussion around security policies • Presence / absence of Security Champions Program • Reward and Contest regarding security behavior and culture including company-wide milestones, etc. • Security-centric special events 	<ul style="list-style-type: none"> • Culture Survey Data <ul style="list-style-type: none"> - Attitudes - Behavior - Cognition - Communication - Compliance - Norms - Responsibility • Proficiency Assessment Data <ul style="list-style-type: none"> - Password & Authentication - Email security - Internet use - Social media - Mobile devices - Security awareness • Others as desired 	<ul style="list-style-type: none"> • Phish-prone Percentage • Industry Benchmarks • Virtual Risk Officer information • Email Exposure Check Data • API integration with other tools

On their own, each of these datapoints are useful, but they are also limited. But the aggregation of several datapoints can be used to paint a powerfully accurate picture of an organization's security culture; and that's where the Security Culture Maturity Model (SCMM) comes in.



Evaluation of CMI Provides Data-Driven Insight into the Maturity of an Organization's Security Culture

As with many maturity models, the Security Culture Maturity Model is loosely based on a Capability Maturity Model (CMM⁶) framework. This model is unique in that it is highly data-driven, based on the insights gathered from KnowBe4's 40,000+ global customers. As with the CMM, the Security Culture Maturity Model has multiple levels, ranging from a level representing very low maturity and progressing up to the pinnacle of achievement. For example, here is the basic structure that most maturity models follow:

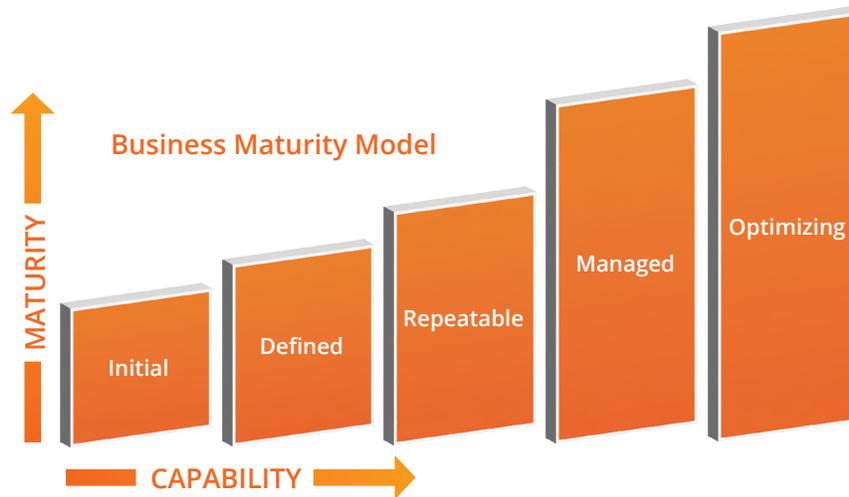


Figure 2: Example visualization of a standard/generic maturity model

And here is another way such models are often represented:

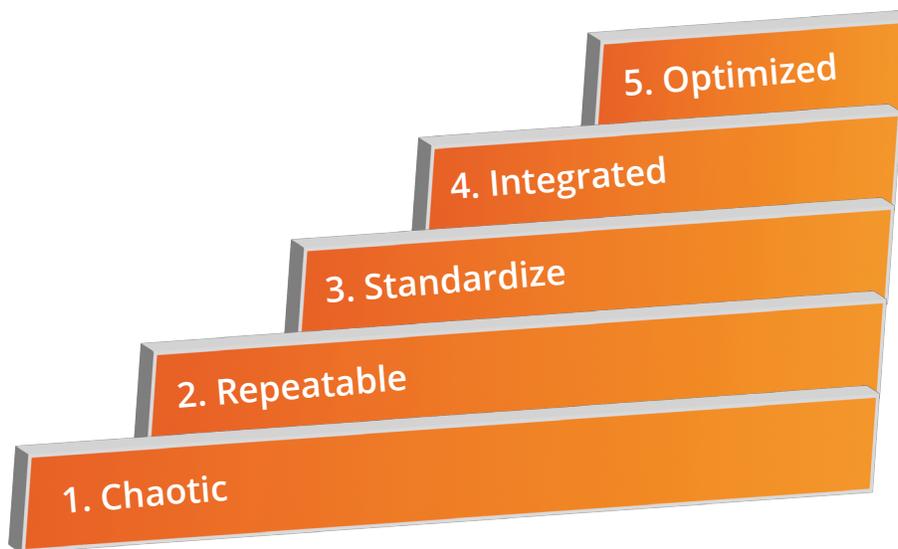


Figure 3: Another common maturity model visualization.

Each of these representations are good at communicating the building blocks of maturity. They are good at showing the high-level concept, but they lack some of the specific granularity that is useful for security leaders.

⁶ <https://stage.cmmiinstitute.com/resource-files/public/dmm-model-at-a-glance>

As such, for the purpose of representing maturity within the context of security culture, KnowBe4 Research proposes the model below:

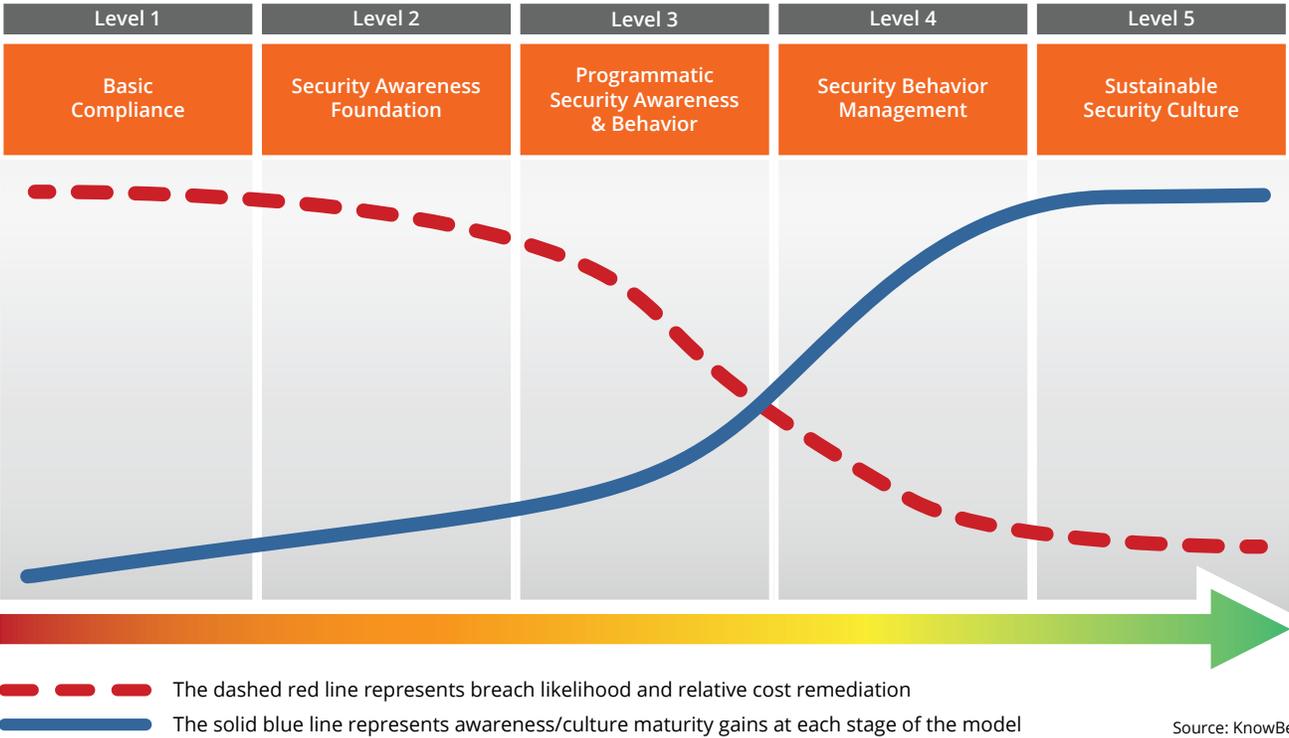


Figure 4: KnowBe4 Research’s Proposed Security Culture Maturity Model

The Model in Detail

The Security Culture Maturity Model is an evidence-driven framework for understanding and benchmarking the current security-related maturity of an organization, industry vertical, region, or any measurable group. It is comprised of five levels. The model’s range accounts for organizations with no formal or intentional awareness, behavior, or culture plan other than to achieve basic compliance (Level 1) all the way up to the most sophisticated organizations who seek to push beyond the pack and are actively working to shape even the unwritten rules and social dynamics of how their employees value security.

An organization’s level of maturity within the SCMM is determined through the automated analysis of the CMIs discussed earlier.

It is important to note that non-KnowBe4 customers can also gain value from the model by using anecdotal evidence to best estimate their maturity.

The S-Curves

One aspect of the SCMM that immediately stands out are the two distinctive S-Curves. Each of these tell a story. The solid blue S-Curve represents the specific awareness, behavior and culture benefits



an organization will achieve at each stage. Notice the inflection points and crossover point for each of the S-Curves. The inflection points and crossover point each represent the real behavioral gains that an organization can expect as they begin to focus on shaping employee behavior through a combination of training, frequent simulations and reinforcement tactics.

Also notice the relationship between the two curves. As security awareness, behavior and culture increase, the likelihood of human-related breach and cost of remediation (the dotted red S-Curve) decrease. And again, there is a sharp inflection point as organizations move beyond knowledge-based awareness and begin intentionally focusing on behavior and the social aspects of how employees value security.

Lastly, there is an additional point reflected in the placement of the curves. There is a gap between the top of the blue line and the top right of the chart, and there is an even more noticeable gap between the very end point of the dotted red line and the bottom point of the final level. These represent a simple truth: no organization will fully “arrive”, and no organization will ever be fully beyond the possibility of experiencing a human related breach. That’s the nature of any security measure, technology-based or human-based. No security layer (technical or human) is able to make an organization 100% secure, but each additional layer of security you add provides additional resilience.

Level 1: Basic Compliance

Organizations at Level 1 have usually been pushed into establishing a security awareness program by regulations, contractual obligations, or because having such a program is seen as an industry best practice.

Organizations here do the bare minimum of training. For example: training based on policies/procedures that are mandated by a regulation or industry standard.

Metrics at this stage are usually focused on collecting the number of employees who have completed trainings, attended security meetings, etc. The program and metrics point to one goal: exposing employees to base-level mandated materials and providing proof that the employees have been exposed to the materials.

The organizational attitude at this level can be characterized as, Let’s just “check the box” and *move on*.

Level 2 (Security Awareness Foundation)

Level 2 represents a significant departure from a compliance-driven program. Organizations here want to do more than the minimum. They understand the value in bringing awareness to threats, best practices, etc. They create resources or find ready-made resources to share as needed. This may also lead them to bring in vendors or create tools to serve their greater awareness needs.

Training is typically conducted during employee onboarding and annually thereafter; however, this level will also often include ad-hoc training, information sharing, or events based on perceived need or benefit.

As organizations mature, they may begin to increase frequency or add more structure around how often they offer training. Similarly, as they progress through Level 2, these organizations generally begin implementing more sophisticated methods for sending relevant information to different audiences and are doing so more frequently. They may begin working with internal marketing and PR departments or they may begin adopting marketing-like practices on their own. These organizations don't stop with required training, they think about sending information out using multiple communication channels, doing more frequent trainings to keep security top-of-mind.

More sophisticated organizations at this level will be considering practices such as segmentation of audiences, role-based and risk-based message targeting and continual messaging/training. They also generally use a diverse selection of content types and lengths that best match the diversity of the organization and the individuality of the learner.

Organizations within Level 2 may also begin conducting ad-hoc phishing simulations as part of an organizational security assessment, however this is generally only done annually or quarterly and is not yet at a frequency to reliably reduce the organization's susceptibility to phishing.



Level 3 (Programmatic Security Awareness & Behavior)

At this level, organizations have tools in place. Their program has much greater structure. They are more intentional about how they choose content, who they send that content to, and the timing involved. Organizations here are also beginning their journey towards driving secure behaviors. They have tools in place for simulated phishing as well as having tools and processes in place for reporting suspected phishing events or other security incidents.

Organizations here are also beginning to focus not only on remediating undesirable behaviors (e.g. clicking on phishing links) but are also proactive about building positive security habits such as reporting suspected incidents, encouraging use of password managers, and more.

Over the past few years, many reports have made much of the fact that the vast majority of breaches

are traced back to human error⁷. This realization has served as motivation for many organizations to begin conducting frequent simulated phishing programs and encouraging the reporting of suspected phish. As such, the majority of organizations we measure are currently at Level 3.

This level is characterized by a pursuit increasing the frequency of training as opposed to annual, once-per-year efforts. At the low end of maturity, organizations are testing and training quarterly. At the high end, they are usually doing some form of training at least monthly, if only for targeted groups.

As organizations climb the S-Curve, they begin to see the real payoff: a measurable decline in risky behaviors. Additionally, this is where the likelihood of, and remediation costs associated with, breach begin to sharply decline.



Level 4 (Security Behavior Management)

Here's some great news, when it comes to influencing behavior, phishing training is just the beginning. It represents only one category of behavior shaping. Approaching security awareness from a behavioral science perspective reveals several possible areas where behavioral interventions can be injected. As organizations pursue more advanced areas of behavior management, they begin to evaluate their policies, procedures, and technologies based on how compatible they are with human nature.

That's where Level 4 comes in. Organizations at Level 4 have made significant behavioral gains, and they are focusing on shifting multiple types of behavior. They are also generally interested in understanding the why behind certain behaviors.

Organizations that approach security with a behavior mindset will have an eye to how their technologies, processes, and policies can begin to work with, or against, human nature to accomplish security goals. For instance, implementing a password manager is a great way to help people up their password hygiene. And finding ways to reward desired security behaviors will help employees know when they are doing the right things and encourage them to do more of those types of behaviors.

Organizations at this level may begin collecting and evaluating behavior-related data across their security stack, their IT ecosystem, and more. They look to data provided from other security tools (e.g. SIEM, DLP, EPP, and others) to determine which behaviors need to be addressed. Behavioral interventions may have been defined for in-the-moment coaching, creating custom training campaigns and events that are as individual as possible.

⁷ <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>

At this point, metrics are generally being used to tell a story that is more nuanced than simply presenting data. Metrics and anecdotes are used to support the human defense and human impact that employees are having within the organization. And employees are being recognized as a critical layer of defense within the organization.

Training at this level could be categorized as continuous. This is all about in-the-moment coaching to remediate, reward, or reenforce behavioral outcomes.

Level 5 (Sustainable Security Culture)

Level 5 is the highest level of maturity. Organizations at this level, intentionally and actively weave security related values, beliefs and behaviors into the cultural fabric of the organization. Specific attention is given to different contexts, use of social pressures, and the knowledge, values and behaviors being reenforced.

Every organization has a security culture. But an organization is only at level 5 when they are intentionally measuring, shaping, and reenforcing culture. This will have elements of compliance, general security awareness and communication methods, as well as behavior management, but all focused toward a larger goal: shaping the organization's unwritten values, norms, expectations, social pressures, and modeled behaviors.

Organizations at this level are working to embed security values throughout the organization and find ways to make their efforts sustainable for the long-term. Evidence of this includes robust behavioral intervention programs, establishment of reward and reinforcement programs, mature "culture carrier" programs (aka Security Champion programs, Security Liaisons, etc.), programs that leverage social pressures, reinforcement, continual messaging, and more.

Security values are woven through the fabric of the organization from the top down. Values are lived out and modeled by established employees so they are seen and can be "caught" by new employees. Security wins (e.g. phish reporting or reporting of other suspicious events) are celebrated. Security issues are viewed as an opportunity to better inform the organization through the use of stories and anecdotes. Security is viewed as a responsibility and a competitive advantage... not a chore.

Training frequency could be characterized as continuous, and a continuous improvement model is associated with the program.



The Value of the SCMM

The SCMM has some interesting properties in that it can communicate at multiple levels. For instance, there is value in being able to quickly communicate what level an organization or vertical is in. There is also value in comparison, allowing an organization to benchmark itself against its industry, organizations of comparable size, region, etc.

This model can be used to communicate at a glance, or in extreme detail backed-up by rich data (as you'll see below). Organizational leaders can visualize their journey and plan the steps required to progress from one level to another. The names of each level are guideposts pointing toward the types of activities that will help the organization progress.

Examples of the Model in Use

The fact that the SCMM is fueled by KnowBe4's dataset gives it immense value. Once this model is formalized and implemented, KnowBe4 customers will be able to gain insights about their maturity that have never before been possible. KnowBe4 Research is formalizing many of the statistical models now, but the insights are extremely interesting.

The Value of Culture Maturity Indicators (CMIs)

Before we show example data, it's important to remember that no single datapoint or test is a fully reliable way of plotting a position within the maturity model. Single datapoints or surveys can provide a good initial guess, but they will always be limited. For instance, an organization might be tempted to look at the SCMM and guess its position based on some of the activities it is currently engaged in, such as phishing simulations. But what if that organization is showing good results with phishing simulations, but their people don't understand some security concepts that are critically important in other areas? The SCMM accounts for this by factoring in multiple Culture Maturity Indicators (CMIs) that can each be weighted and averaged before the model computes a final score and maturity level.

Some of the CMIs that could be factored in include:

- KnowBe4's Security Culture Survey (SCS)
- KnowBe4's Security Awareness Proficiency Assessment (SAPA)
- Phish-prone Percentage (PPP)
- Use of phish reporting buttons
- Accuracy of detecting phish as determined via KnowBe4's PhishER product
- Number and types of training modules taken
- Behavioral data collected from security technologies (e.g. SIEM, DLP, etc.)
- Other collected behavioral data (input or collected)
- Configurable booster scores

The accuracy of the model in showing an organization true maturity grows as each CMI is factored in. In other words, accuracy increases as the number of datapoints increase.

Here’s an example. This one uses two CMIs, specifically the Security Awareness Proficiency (SAPA) Assessment and the Security Culture Survey (SCS). The example is useful in understanding the current distribution of organizations across the model. Each of these on their own would have limited directional accuracy; but when combined, they serve to add precision.

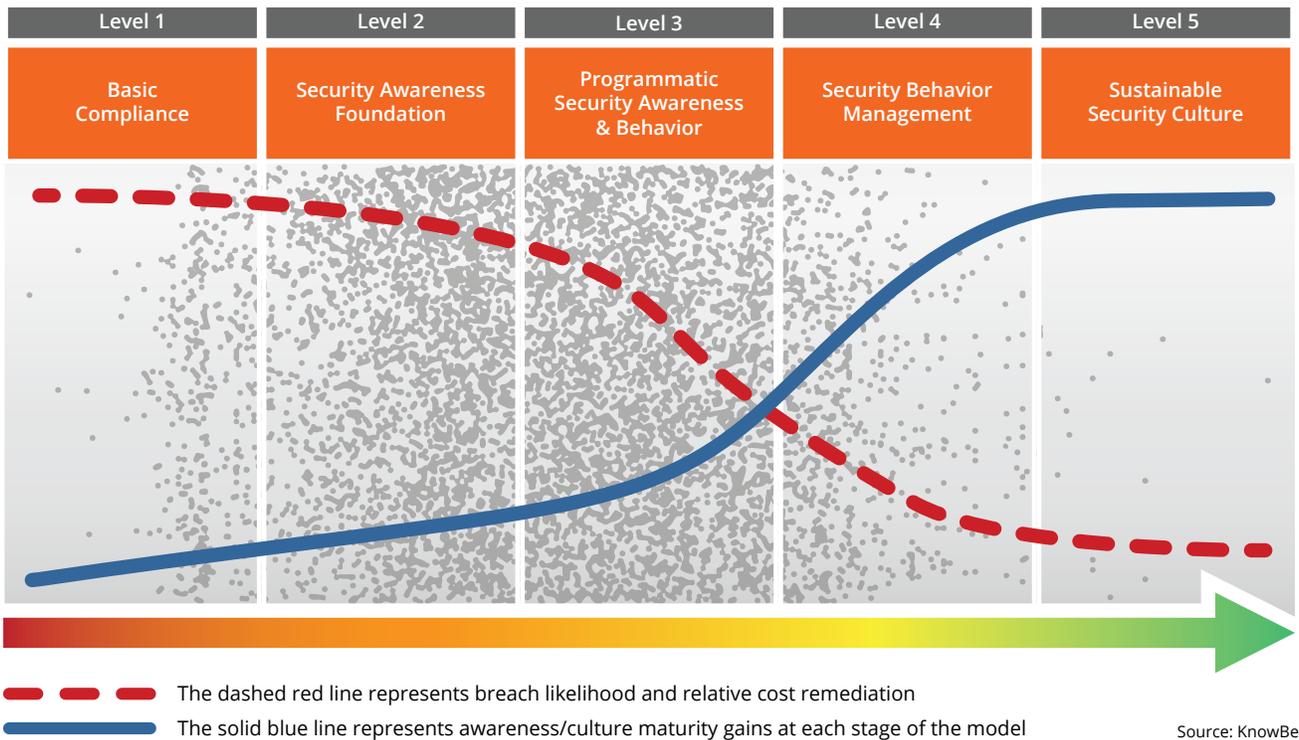


Figure 5: Example of the SCMM showing maturity across organizational scores with KnowBe4’s Security Awareness Proficiency Assessment and Security Culture Assessment as CMIs

This is a prototype result based on real data, presented for illustrative purposes. In future research, more CMIs will be added to these models. Doing so will impact the distribution. Our team is currently working through the statistical modeling and various CMI weightings to provide the best representations possible. In other words, lots of cool stuff is ahead!

Here’s another illustrative example. Whereas the last example was across several thousand organizations, this one focuses in on a single organization and shows how multiple CMIs provide context. This example shows an organization whose information sharing program is really only focused on doing the minimum. But they also engage in monthly phishing simulations and have been making good progress. Additionally, they sent out an awareness survey that returned its own assessment of their maturity, and they have some security technologies reporting observed behaviors.

The CMIs used in this representation are as follows:

- **Basic awareness program:** If this were the only input, this organization would be at level 2.
- **Security survey score:** The results of this organization’s security awareness assessment (on its own) would lead a model to believe they were in level 3.
- **Phishing program structure and results:** Strong results would indicate level 4.
- **Other observed behaviors:** Bringing in other observed behaviors (e.g. password hygiene and document sharing) provided evidence that this organization is in level 3.

Current Maturity Given Available Data = Level 3

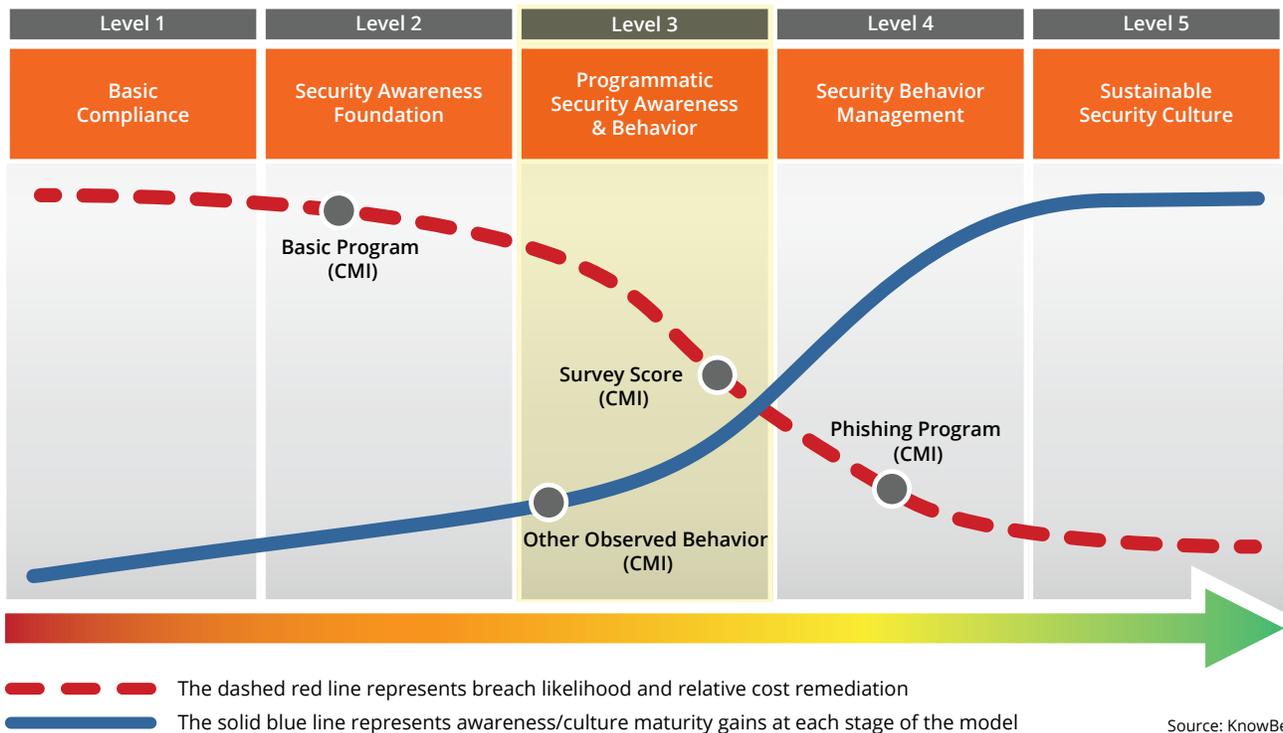


Figure 6: Example of the SCMM multiple CMIs of a single organization before arriving at the composite/average SCMM level.

Each of these CMIs, on their own, provide only part of the picture. But, by looking at multiple CMIs, and because each CMI will have an associated weighting, the model will much more accurately arrive at an organization’s score and maturity level. In this instance, the model would place the organization at level 3, “Programmatic Security Awareness & Behavior” because that’s the aggregated score achieved by evaluating the available CMIs.

Other Ways of Using the Model

Another way the model can be used is in a more “unplugged” mode. This is how most non-KnowBe4 customers can leverage the SCMM. They can aggregate several of their own representative CMIs and anecdotes, and then use the model’s maturity level descriptions as a guide.

The goal is to provide a model that is usable by the entire industry, not just KnowBe4 customers. Over the next few months, KnowBe4 Research will release more information related to the CMI's most associated with each level. Additionally, the team is planning to release some easy to use questionnaires organizations can use to get an idea of their current maturity level and what steps they can take to progress to the next level(s).

Refinements to Come

This model will evolve over time. KnowBe4 is dedicated to continually tuning the statistical models, available CMI's and their weightings, and more. As the industry matures, it is likely that adjustments to the thresholds needed to move from one maturity level to another will also be refined. Culture is a moving target. As threat actors evolve, countermeasures do to. This directly influences security culture, and an evidence-based model that keeps being updated will ensure a more accurate representation of the real world. This could mean that achieving a particular maturity level (or even staying at a specific level) can become progressively more difficult in years to come as the general maturity of all measured organizations slowly improve.



Additional Resources



Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test



Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization



Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click



Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do



Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com