HOW TO REDUCE HUMAN RISKS IN CYBERSECURITY WITH

THE SAFE PROGRAM

BUREAU VERITAS

Secura
A BUREAU VERITAS COMPANY

According to the Verizon Data Breach Report, 82% cybersecurity incident breaches in 2022 involved a company employee and this number is increasing considerably year after year. Cybersecurity attacks have major and sometimes existential impacts on organizations, including financial loss, customer credibility damage and long periods of recovery.

The human factor plays a significant role in cybersecurity and in many cases forms the weakest link of an organization´s cyber defense. While many organizations focus on their technology and processes, in the end, attackers often succeed by exploiting human errors.

To become resilient against cyber attacks, organizations must focus on increasing the resilience of people, processes and technology within cybersecurity.

For more effective protection against human error, Bureau Veritas combined the expertise of security specialists with the expertise of psychologists to develop the **SAFE Program (Security Awareness For Everyone Program).**

This program, based on the MOA-model, has a single goal - effect behavioral changes to **increase the human defense against cyber attacks.**

CONTENT

P 3 Understand what is beyond behavioral change

P 4 Why the MOA Model supports behavioral change?

P 5 How the SAFE Program will reduce cyber risks in your organization?

P 6 Let's dive in the E-Learning library

P 7 The E-Learning library content

P 8 Why The SAFE Program works?

P 9 A sense of urgency?

UNDERSTAND WHAT IS BEYOND BEHAVIORAL CHANGE

In light of this information it is important to understand the reasoning of employees and raise the question of what drives individuals to behave safe. Behavioral change is not a new subject in the field of psychology and many experts have been working on the topic for decades. ***The research shows that even if someone is aware of what they should do, they will not necessary do it.*** There are hundreds of examples of this visible in daily life – like breaking traffic rules, no quitting smoking, or disregarding hygiene measures. In cybersecurity, an example of common unsafe behavior is people who know that they should have strong passwords, but the average password strength remains very weak in most organizations.

WHAT DRIVES HUMAN BEHAVIOR

Often, people know what they should do, but end up doing something different. We know that we shouldn't text while driving, cross while the light is red or eat too much candy, but we still do it. In our daily life there are thousands of examples just like these.

It shows that only being aware of the correct behavior doesn't mean that you will actually do it.

Most people know that they should have strong password, however the average password strength is very weak in most organizations.

FOCUSSING ONLY ON AWARENESS WILL NOT CHANGE PEOPLE BEHAVIOR

Therefore, we define a clear gap between awareness and behavior and this is also the case within the realm of cybersecurity.

The message here is that only focusing your efforts on awareness won't change the behavior of anyone. On the contrary, what will change behavior is focusing on lifting barriers and making sure that the end goal of policies and interventions is behavior.

BEHAVIOR CHANGE

ABILITY

Ability refers to what a person knows and understands about security and about the risks. This is the factor that is most focused on in current approaches such as E-Learnings, new rules creation and classroom trainings.

MOTIVATION

In addition to knowledge, behavior is determined by motivation: is someone willing to perform the behavior? Motivation is the result of various personal factors such as experience (has someone tried it before and how did it go?), attitudes (is someone prepared to do some extra effort in return for more safety), perception, norms and values.

OPPORTUNITY

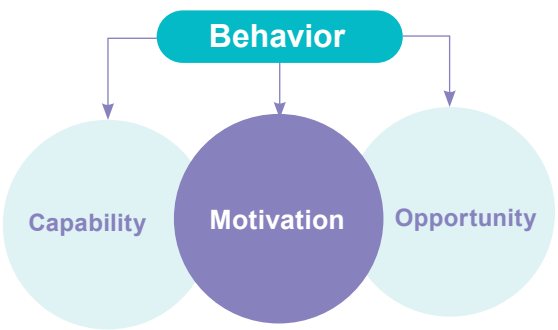
The third factor that determines behavior is opportunity: are people enabled to perform the desired behavior? Opportunity is determined by organizational factors. Context and culture are the most important here. The culture of an organization has a major impact on the behavior of employees.

WHAT DRIVES HUMAN BEHAVIOR

Psychologists have long known that behavior can be explained in a multitude of ways. One of these ways is the MOA-model which explains that a certain behavior only happens when a threshold of **ability, motivation and opportunity is reached** (O¨ lander & Thøgersen, 1995).

Finding out what the barriers are for behaving safely is central for a good cybersecurity approach within organizations. **Only by researching these barriers can you create focused interventions that actually change behavior.**

THE MOA MODEL

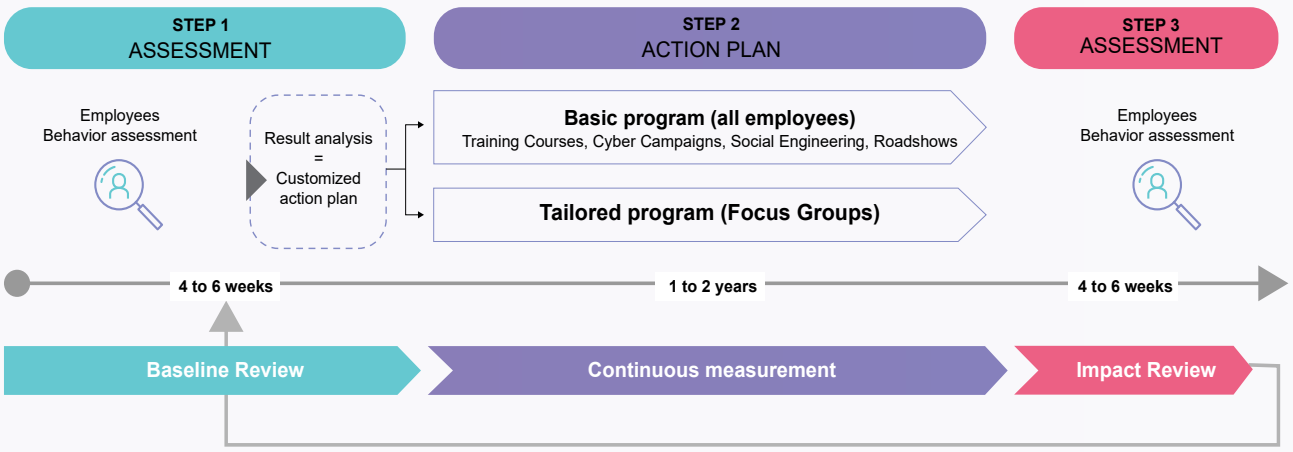


HOW THE SAFE PROGRAM WILL REDUCE CYBER RISKS IN YOUR ORGANIZATION

For more effective protection against human error, Bureau Veritas combined the expertise of security specialists with the expertise of psychologists to develop the **SAFE Program**. This program, based on the *MOA-model*, has a single goal - effect behavioral changes to ***increase the human defense against cyber attacks.***

This full security behavior program focuses on assessing, enabling employees to become more cyber resilient and measuring in a continuous way the impacts on behaviors.

The 3-step approach of the SAFE program



STEP 1

BASELINE REVIEW

The **SAFE Program** will start with a kickoff meeting and workshops with your internal team to define the goals to reach in term of security awareness as well as the communication campaign to set. Once done, we will proceed with a baseline review where we will measure employees behavior regarding ability, motivation and opportunity. It is based on a variety of methodologies and goes further than a simple survey. The outcomes provide a clear insight into the current status and into which of the factors require extra attention. All this information will allow us to create your SAFE custom action project plan to launch.

STEP 2

ACTION PLANS & CONTINUOUS MEASUREMENT

This step consists of a **Basic Program** for the entire organization in which all three factors of behavior receive repeated attention: keeping the necessary knowledge up to date, boosting motivation and establishing the right culture. This is done in various ways such as social engineering, road shows and training through our extensive E-Learning library. Our library offers courses on various topics : Introduction into cybersecurity, phishing, malware and data privacy as well as specific modules for specialists and managers.

In addition to the basic program, a **Tailored Program** runs every quarter with a focus group. Specific goals are defined as well as concrete interventions. One of the distinguishing features of the SAFE program, is that it does not jump to solutions. Instead of assuming what would help the employees most to behave securely, we put considerable effort into understanding them and it starts with identifying the barriers and then working to remove them. The result of this step will provide insight in what is currently withholding people from acting in line with the goals.

STEP 3

IMPACT REVIEW

To measure the effects of the program, we conduct a deeper measurement at the end of a first year. The results will help to define a new action plan for the coming year as well as bringing to your organization an updated view of the behavior improvement.

LET'S DIVE IN THE E-LEARNING LIBRARY

Ability is a critical element of the MOA-Model of behavioral change and corresponds with education, awareness and knowledge. An employee is not able to act if they do not know what they should do. Therefore, our SAFE Program prioritizes ensuring employees have the necessary knowledge.

This knowledge is typically delivered via E-Learning courses. Bureau Veritas has developed 31 security awareness modules available off-the-shelf in 7 languages that can be deployed immediately. Typically, we support our customers to identify which of the courses are most relevant to their teams and structure a deployment plan that allows continuous learning without being overwhelming.

SPOTLIGHT

- With real-life situations, catchy examples and interactive exercises, you will work in a step-by-step manner towards achieving behavioral change.
- The Library is designed with a pedagogical approach that focuses on learning, practicing and anchoring knowledge.
- E-Learning courses contribute to ISO 27001 and TISAX compliance controls for employee education and awareness.

SAFE E-LEARNING LIBRARY

THE E-LEARNING LIBRARY CONTENT

	Phase 1	Phase 2	Phase 3
SECURITY TOPICS	**LEARN**	**PRACTICE**	**ANCHOR**
INFORMATION SECURITY	Introduction to information security (19 min)	Clear desk, screen & office (8 min)	Ransomware (1 min)
	Cybersecurity for executives (8 min)	Strong Passwords (3 min)	Use of Passwords (3 min)
		Report Security incidents (3 min)	Report information security incidents (3 min)
INFORMATION CLASSIFICATION	Information classification (10 min)	Information classification (4 min)	How is information classified? (3 min)
DATA PRIVACY	GDPR (12 min)		Privacy in practice (4 min)
PHISHING	Phishing (11 min)	Phishing (3 min)	Know with whom you are dealing (1 min)
MALWARE	Malware (6 min)	Malware (4 min)	
MOBILE DEVICES	Mobile devices (5 min)	Bring your own device (4 min)	Secure your mobile devices (3 min)
THE NEW WAY OF WORKING	The new way of working (8 min)	Social media & working in cloud (4 min)	Internet of Things (IoT) (7 min)
		Working in public places (4 min)	Work securely outside the office (3 min)
SOCIAL ENGINEERING	Social Engineering (7 min)	Social Engineering (4 min)	
RISK MANAGEMENT	Risk Management (10 min)	Access control (4 min)	
OPERATIONAL TECHNOLOGY SECURITY	Dilemma's in OT Security (25 min)		

For more detailed information, please download "The safe program e-learning library content"

WHY THE SAFE PROGRAM WORKS?

With the **SAFE approach, your company will invest in creating awareness** and achieving behavioral change that is tailored to the needs of the employees in your organization.

As a result, the maturity level of information security increases, making the organization more resilient against outside attacks.

By choosing **The SAFE program**, it is also measurable and clear, both internally and externally, that privacy and information security are of great importance to you.

SAFE demonstrates to make your employees more aware and competent to behave appropriately in case there are attempts by malicious parties to gain access to systems and information.

With SAFE, your employees reduce the chance of cyber incidents with a major impact and thus the associated high costs and the risk of reputation damage.

KEY TAKEAWAYS

- Designed by psychologists and information security specialists.
- Focused on safe behavior as end goal so it goes beyond awareness.
- Focused on all aspects of behavior: in addition to ability (knowledge), also motivation and opportunity.
- Tailored to the nature and risks of an organization (so no "one size fits all").
- Developed on the basis of psychological techniques for behavioral change such as stimulation and facilitation and goes beyond traditional training.
- Based on repetition, so no "one-time check-in-box activity".

A SENSE OF URGENCY?

Finally, how is it possible that after years of investing in cybersecurity defenses, still one phishing email can lead to a potential incident of a business at risk?

Technical software and procedures have been in place for years but still companies are facing issues with this initial point of access by hackers. Are companies unsuccessful in training their staff or are attackers getting more sophisticated?

It could be the first answer, as one of the trends in cybersecurity for 2022 is according to Gartner*, a shift from traditional security awareness training towards an approach that is beyond compliance-based awareness campaigns and focused in holistic behavior and culture change programs.

That implies that the current efforts on training employees on recognizing cybersecurity threats is not enough. Especially when looked at the key numbers of the human factor, one can imagine that this factor needs more attention.

Bureau Veritas will support your organization to develop a safe culture. By developing the resilience of your employees, you will intensively reduce human risks in Cybersecurity. Take action and reach out our experts now!

*https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

SHAPING A WORLD OF TRUST

Bureau Veritas is a Business to Business to Society company, contributing to transforming the world we live in. A world leader in testing, inspection and certification, we help clients across all industries address challenges in quality, health & safety, environmental protection and social responsibility.

For more information,
contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE
bureauveritas.com

BUREAU VERITAS
1828

BUREAU VERITAS

Shaping a World of Trust