Hewlett Packard Enterprise

Business white paper

Awareness is only the first step

A framework for progressive engagement of staff in cyber security

Table of contents

Achieve lasting behavior change

Security communication, education, and training (CET) is meant to align employee behavior with the security goals of the organization, but it is not always designed in a way that can achieve this.

Currently, security CET is mostly delivered as generic web-based training with security quizzes, a "box-ticking" exercise that only indicates employees have read through pages and know the answers to questions. It does not mean they will adopt secure behaviors as they go about their daily tasks.

The lack of reliable indicators means senior management does not know if recommended security behavior is actually followed in practice. In modern organizations today, employee attention and efforts are consumed with messages about health and safety, sustainability, sector-specific regulation, and security. All of these are secondary activities that take time and attention away from primary productive activity. Since current CET often recommends behaviors that conflict with productive tasks, it is ignored—just part of the background noise of a multitude of corporate messages.[1]

The purpose of this paper is to set out a framework for security awareness that employees will actually engage with, and empower them to become the strongest link—rather than a vulnerability—in defending the organization.

The first essential step is security hygiene—ensuring recommended security behaviors can be adopted by employees engaged in productive activity. To achieve engaging security CET, security knowledge and skills must be tailored to specific groups of employees, and deliver a core set of security skills that are relevant to their productive tasks. It is unrealistic, and a waste of company resources, to try and mold every employee into a full-fledged security expert.

This paper should serve as a guide to creating interactive, dynamic, and engaging programs that give the right knowledge and skills to match individual roles. These programs should be creative and fresh, and most crucially, adapted to regional and national cultures.

Untargeted content and unrealistic demands reduce the lasting effects of CET messages within an organization, and the willingness of employees to take an active role in protecting the organization's information assets. That's why each organization needs to identify specific behavior goals and take baseline measures before implementing it.

A set of steps, required to deliver effective security CET as a natural part of an organization's engagement with employees at all levels, is outlined. Depending on different needs, many vehicles are available from security games, quizzes, and brainteasers—and possibly prizes—to encourage employees to test their knowledge and explore in a playful manner.

The most important output is that different approaches are needed for routine security tasks, and those tasks require application of existing security skills to new situations. There are so many creative ways to improve security behaviors and culture. The secret is engaging your people in the right way, so they can convert learning into tangible action and new behavior. Security CET needs to be properly resourced and regularly reviewed and updated to achieve lasting behavior change.

[1] "From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance," Information Security Forum (ISF), February 2014

Make it appropriate
Training should be aligned with risks. This relies on monitoring or good situational awareness. An example is talking on mobile phones in a public place, such as public transportation.

Ensure it's regular
This implies a controlled cycle, informing staff of security issues that relate to them and the work they do. Without measurement and continuous improvement, awareness campaigns cannot be effectively targeted and refined for specific audiences. This can lead to a loss of impact, saturation of attention, and higher costs in maintaining awareness materials.

Be relevant
Training should be aligned with tasks that employees perform as part of their job. Without recognizing what is reasonable to ask of people, while also satisfying the demands of their primary role, expectations around security can increase toward security responsibilities becoming a full-time job in their own right.

Engage your employees

Most employees in modern organizations interact with information and technology that is essential to the functioning of the organization. If they are not able or willing to protect these assets, the organization is at risk. To engage employees to participate in protecting these assets and provide them with the skills needed to do so, organizations use security CET.

Responsibility, trust, communication, and cooperation are the four cornerstones of an engaging security culture. So, it's necessary to use an approach that motivates employees to play an active role in corporate security. Employees should understand what to protect, why they should want to protect it, how the organization can help them with this, and how successes and mistakes can be used as opportunities to learn and improve.

The ISO27001 standard drives many information security programs. The standard recommends increasing user security awareness. But it stops at suggesting how this should be achieved, other than to say that individuals "receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function" (section A.07.02.02).

The human element plays a significant role in the successful delivery of security in today's organizations. Security behavior is greatly influenced by employees' personal perception of risk. These perceptions can be changed.

Information security is a "wicked environment." It reacts to people's actions and is constantly changing.[2] An organization's goals, culture, and technologies change over time, too. As the threat landscape continuously changes, security knowledge and skills among novices, and even among experts,[3] need to evolve constantly.

Most employees are not hired or remunerated for their security expertise, but for their contribution to the organization's primary business. Employees are focused on performing their primary role—especially when remuneration is linked to productivity.[4] This means most employees will not adopt security behaviors that severely hamper their performance on primary tasks.

Before mandating a security behavior, your organization needs to ensure that behavior can be complied with, without routinely blocking productivity—a step called security hygiene.[5] Once that's ensured, security CET communicates correct behaviors and builds skills needed to further target risks that are relevant to different groups of employees.

[2] "Using behavioural insights to improve the public's use of cyber security best practices," Lynne Coventry, Pam Briggs, John Blythe, and Minh Tran; Government Office for Science, London, UK, 2014

[3] "More is Not the Answer," Cormac Herley, IEEE Security & Privacy Magazine, 2014

[4] "Human Vulnerabilities in Security Systems," Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P.; In Human Factors Working Group White Paper, Cyber Security KTN Human Factors White Paper, 2007

[5] "From Weakest Link to Security Hero: Transforming Staff Security Behavior," Shari Lawrence Pfleeger, M. Angela Sasse, and Adrian Furnham; Journal of Homeland Security and Emergency Management, 11 (4) 489–510, 2014

Permanent employees and contractors Contractors have occasional or limited-term presence in an organization, and use a subset of its facilities. They do not have the same opportunities to learn new skills and are less likely to see posters and leaflets displayed around the premises. Contractors need in-time training that is refined to their limited role within the organization; they won't necessarily have the time or need to develop the same range of security behaviors that employees do.

Learn how organizations approach security

Currently, CET activities try to raise awareness among employees through distinct, dedicated training programs at regular intervals during employment. Content can be a mix of potentially relevant and irrelevant information, depending on how much attention has been given to the requirements of different roles, existing competence or context, and regular use.

Employees—and where relevant, contractors and third-party users—are generally trained on organizational policies (and updated) on a regular basis. But does the fact that training is given regularly mean it's effective? Skills can be learned through repetition, but are they the right skills for the right people?

As covered,[6] a tick-box approach, however thorough, only indicates that employees have had the opportunity to become informed and can recall immediately afterward what the correct answer is. There is no guarantee that they carry advised behaviors into practice. Humans are not computers that replace an existing behavior with a new one immediately, and not all people internalize and use skills in the same way. The expectation that behavior will improve if users know the facts is not correct. The problem appears to be a mistaken attitude toward proven security practices such as computer-based training (CBT), with limited evidence to support its effectiveness or efficiency.

CBT is a self-directed online learning process that enables flexibility of location, time, and topics. Topics typically include protection of information—such as a password or use of social media, response to security-related events including spam and phishing, and recognition of social engineering threats.

To fulfill its purpose, CBT should achieve lasting, positive change in the attitude and mind-set of employees toward security. It should be clear that the organization's security policy and prohibited behaviors are vital to protecting the information assets and technology infrastructure of a company. Advice should be seen as an enabler that supports the organization's goals.

Improve current approaches

Current CBT approaches are far from efficient.[7] Research at UCL,[8] found that engaging directly with employees to understand their perception of security in their jobs and the workplace, indicated the following:

Maintain relevance—Training should be ongoing as the organization changes and employees move into and across roles, with a focus on what is necessary for their jobs.

Plan for learning to happen naturally—Repetition of new skills reinforces learning, but training should not overwhelm employees with information or take up excessive paid work time.

Give thought to the overall package—A joined-up approach for communicating security awareness within the organization provides internal consistency and measuring progress for targeting remediation activities if training is insufficient.

Share the enthusiasm—CET should be creative, fresh, and targeted to employees' working practices, where an interactive element further involves the individual.

[6] "From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance," Information Security Forum (ISF), February 2014

[7] ibid

[8] "Learning from 'Shadow Security': Why understanding noncompliance provides the basis for effective security," Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse; Workshop on Usable Security (USEC), 2014

Think differently about security behavior

Since communication and training need to be targeted to organizational risks and employee groups, there is no shortcut to developing an effective security awareness program. Each company, like yours, must define for itself the security culture it seeks to promote. If there is no visible effort to do so, it sends the message to employees that the organization is not serious about security.

That's why there is a need for a new way of thinking: static, general computer-based information security training packages do little to influence employee behavior. To be effective, security training must be based in the work context and address specific security needs, with regular ongoing reminders of the key messages. Awareness campaigns should be tailored to employees' needs—see Figure 1.

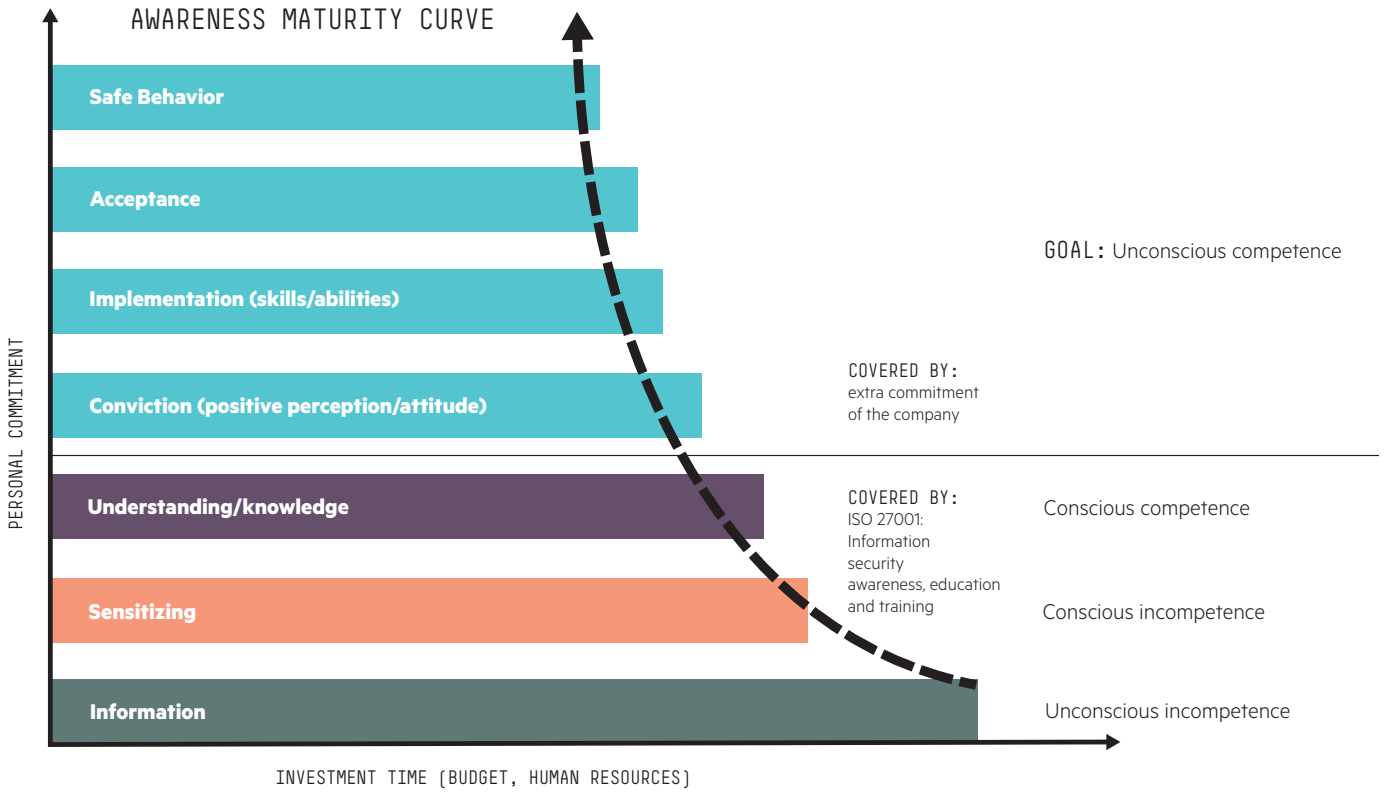

Figure 1: Hewlett Packard Enterprise Awareness Maturity Curve

Many organizations only invest as much as the ISO standard suggests, not recognizing there are more steps required for awareness campaigns to be effective.

Figure 1 indicates that in order to change security behaviors, a company needs to invest in the security knowledge and skills of its employees. Progress is not automatic: Every step toward the goal requires different activities.

Effective awareness requires consistent communication through several channels (the Information and Sensitizing stage on the curve). The messages delivered by a computer-based training program must be supported by consistent, accessible wording on posters and in newsletters. The objective of the communication measures should be to achieve an

unconscious competence in employees—that means being adequately prepared for security risks and tasks. As opposed to having an unconscious incompetence, which reflects lack of ability due to missing knowledge and skill transfer.

For the Understanding and Conviction stages on the curve, management must be genuinely involved. An employee´s motivation is the result of the sum of interactions with management—when it comes to security behavior, management must give aligned messages in team talks, AND lead by example. Conversely, senior management, seeing themselves as "too important" to comply with correct security behaviors will signal that the organization is not serious, and "poison" the security culture.

In the Implementation stage on the curve, the emotional level should be addressed. Security roles should be assigned so employees develop a personal responsibility for the organization's protection, and to give security an identity.

The last two steps, Acceptance and Safe Behavior on the curve, rely on the commitment of employees to the organization—their willingness to practice their skills over time. There is know-how for transforming behavior to be self-sustaining. It is important to examine the lived security culture (not just policy documents), look for weak spots, and identify needed behavioral changes.

Management needs to support the acquisition of security knowledge and skills by acknowledging and praising correct behavior. Awareness can be fostered easily by systemic communication. That means it's about empowerment—the classification and practice of security-compliant actions. It is a requisite to engage with employees to foster social competency and develop a dialogue around security.

Achieve unconscious competence

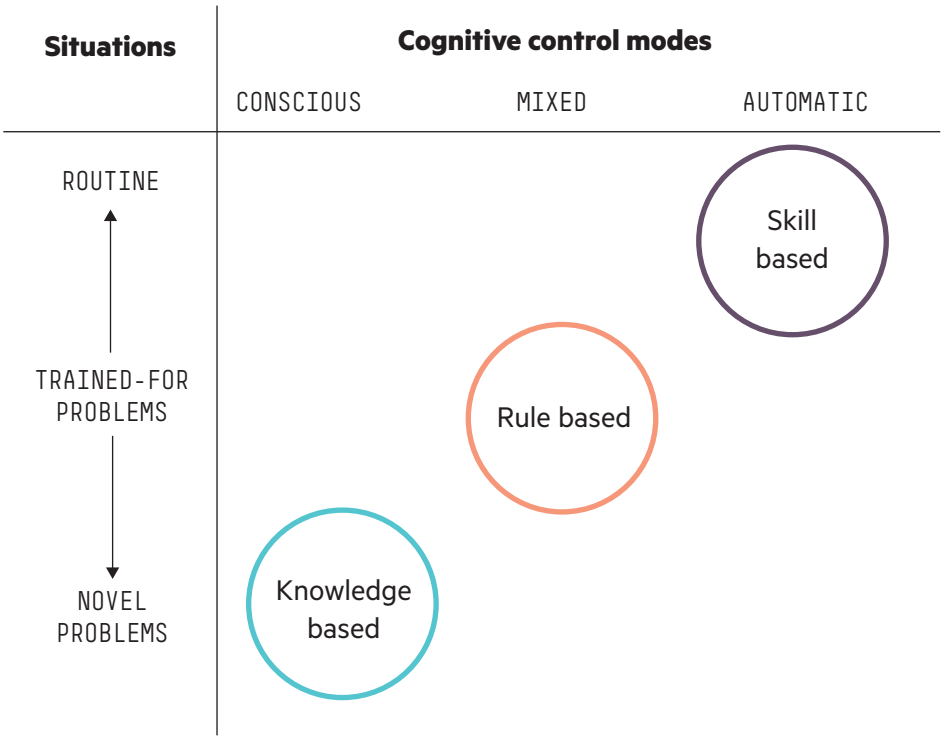

Figure 2: Three levels of performance control[9]

[9] "The Human Contribution," James T. Reason, Burlington, VT: Ashgate, 2008

Incompetence and human performance—Incompetence needs an explicit response from the organization. Human performance begins at the knowledge-based level (see Figure 2), relying on inner dialogue or the instruction of others.[10] This is flexible, but error-prone. Robust, dependable technical controls can compensate for unconscious incompetence—a lack of developed training or skills—of employees, but only up to a point. This approach does not engage employees emotionally, or build skills required to deal with novel security problems. Where conscious incompetence exists, employees need be encouraged to reconnect with security.

Unconscious competence and trained-for problems—Unconscious competence applies to routine, well-understood, security-related tasks. Instructions must achieve a clear goal that does not prevent completion of the primary task. Routine security tasks—as learned sequences of actions—are assumed to manage all possible outcomes in the scenarios to which they are applied, to the satisfaction of the organization and its security policy. When this is not the case, and gaps are encountered in policy or coverage, employees resort to slow, cumbersome—albeit powerful—conscious control.

Conscious competence and novel problems—Conscious competence is key in novel situations that are not well understood. Individuals have to adapt elements of learned behavior or personal experience to approach a security problem. This may leverage skills from the productive task, such as deciding what information can and cannot be spoken aloud when holding a phone call in a public space. Reliance on conscious or unconscious competence may also differ according to the pervading security culture—individuals may be permitted autonomy in some cases, or instructed to delegate decisions to superiors or other proxies.

Security awareness and the relationship between employees and the organization

In addition to formal employment contracts, organizations manage employee behavior through informal psychological contracts, whose nature depends on the company and its structures. For example, most organizations make it clear that sexual harassment or racial abuse will not be tolerated, without specifying every single behavior that would be part of the category. The power of psychological contracts lies in the knowledge that fellow employees will notice wrong behaviors and disapprove, as much as the risk of detection and disciplinary action by the organization.

Security is currently not part of the psychological contracts in most organizations. Once the organization has identified the assets and ways of protecting them, and ensure that they can be followed (security hygiene), doing the right thing by security can also become part of the psychological contract with employees.

One objective of the company should be to explain security topics in the context of the company and communicate them.

Employees should want to help the organization, and the organization should help employees by targeting security awareness to relevant employee groups, and prioritizing the most important behaviors. Doing so will be particularly effective when employees identify strongly with the organization's goals and success. Management should provide an energizing culture of leadership in which employees can excel and develop a sense of loyalty. A high level of identification and loyalty, together with a psychological contract, provides a strong basis for discouraging misconduct or careless behavior by employees.

It is important that management strives for constant support and improvement: It should solicit feedback and act on it, developing a way of tracking indicators of participation. As far as honest mistakes are concerned, it should develop a no blame culture, and create an environment in which mistakes and near misses are analyzed—an important aspect of safety management[11] that security has yet to adopt. The will of employees to improve security behavior must be matched by the organization's will to constantly improve the way it manages security.

[10] "The Human Contribution," James T. Reason, Burlington, VT: Ashgate, 2008

[11] ibid

Security and productivity

Security effort—Today, we observe many conflicts between security and productivity in the working environment. Employees routinely have to complete security tasks that block or disrupt their primary tasks. If security is not a natural fit to an employee's job, the security effort becomes a nuisance. If security is visibly and obviously aligned with the organization's goals, employees can recognize a natural fit with their productive tasks.

Employees may still comply because of goodwill toward the organization, but eventually their compliance budget will be exhausted.[13] If security gets in the way of employees' primary job, they are more likely to develop a negative attitude toward the organization's culture.

Security and productivity—Individuals will rationalize any competition for their finite effort—existing between security and their primary, productive task. Asking for too much attention and effort reduces the impact of communication; even when employees comply with security, although they don't know why. Regular, two-way engagement with employees can foster a shared understanding and sustainable balance of where security fits with productive tasks.

Security, productivity, and cost—For the organization, there is an interplay among security, productivity, and cost, such as help desk support. There is a balance to be struck; considering the bigger picture of security provisioning can ensure a more harmonious working environment.

It can also be useful to motivate building of security knowledge and skills by making a connection to personal use of IT. For instance, where remote working is allowed, provide a secure home router that can also be used for personal purposes.

Scenario-based security behavior engagement

UCL conducted empirical research[12] on how security and security behaviors fit within the work day, through interview and survey tools that directly engaged employees within organizations. This approach identifies the causes of unsecure behavior and helps managers understand how security communications and training initiatives should be targeted to transform them. If employees say it is difficult to comply with security policies, this represents an opportunity for improving policies and mechanisms, rather than a transgression that must be punished.

This method is based on the premise that self-reported behavior is a good indicator of actual security behavior, although there's a likeliness to under-report noncompliance rather than over-report it. Engaging directly with employees assists in identifying the entry-points for security within a person's work routines. Relating security to the primary role as a collection of supporting tasks also supports dialogue with other stakeholders with competing interest in shaping the way people behave within the organization, including safety and human resources (see also psychological contracts).

Current research here is illustrated in interviews conducted to understand the role of security in employees' working lives.[14]

Use a framework for progressive engagement

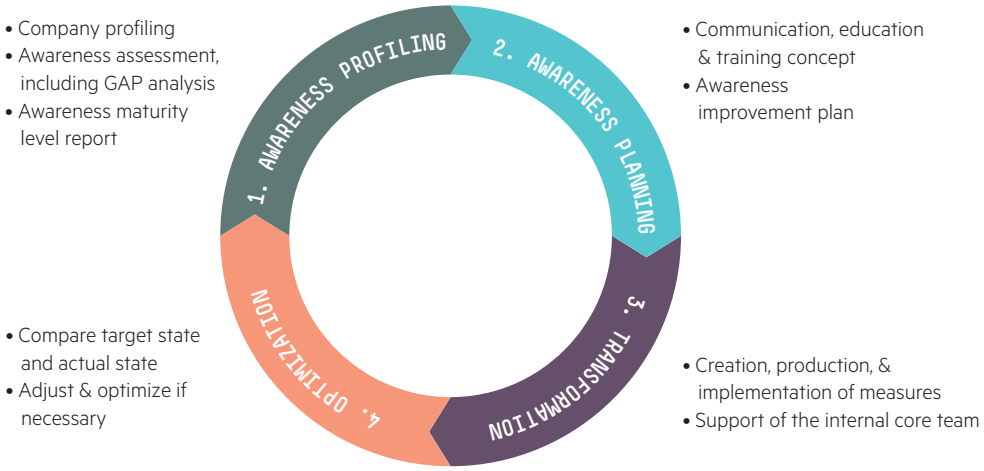

Figure 3: Progressive Engagement Framework

A combined framework, consisting of four steps, acts as a lifecycle for the awareness activities that need to be implemented and revisited over time:

Awareness profiling

A profile of the organization is created, including the scope of the campaign and desired target state of it. Since every organization is different, relevant factors need to be measured. There are different kinds of qualitative and quantitative methods for assessment.

[12] "Learning from "Shadow Security": Why understanding noncompliance provides the basis for effective security," Iacovos Kirlappos, Simon Parkin, M. Angela Sasse; Workshop on Usable Security (USEC), 2014

[13] "From Weakest Link to Security Hero: Transforming Staff Security Behavior," Shari Lawrence Pfleeger, M. Angela Sasse, Adrian Furnham; Journal of Homeland Security and Emergency Management, 11 (4) 489–510, 2014

[14] "Learning from "Shadow Security": Why understanding noncompliance provides the basis for effective security," Iacovos Kirlappos, Simon Parkin, M. Angela Sasse; Workshop on Usable Security (USEC), 2014

Deviation between the current and desired security awareness state is identified, as are any security provisioning elements acting as obstacles to healthy security habits. The results are recorded in a Security Maturity Level Report.

Awareness planning
An economics-based approach to improvement would, as a first step, remove or revisit any problematic—or majority of employees'—measures (per security hygiene).

In the CET concept, the objectives, responsibilities, and overall steps need to be defined. Awareness improvements are prioritized according to relevance and determined in a project plan where measures are defined in more detail.

Transformation
In this phase, initiatives are put into practice through security awareness involvement activities (see the next section). This includes the production of attractive security gimmicks.

Optimization
If the target state has not been reached, additional improvements can and should be made iteratively. Optimization can include revisiting the results of any security hygiene exercise(s)—good-intentioned improvements have the capacity for unforeseen implications.

Transform awareness and involvement

General campaigns that repeat standard security advice—such as have strong passwords and be aware of phishing—do not work. Each company has to be evaluated and a specific campaign with individual initiatives created. It can be argued that these initiatives are more involved than actual interventions.

Phased introduction of involvements should be based on the results of the awareness assessment and should transform security behaviors according to the security culture, which should align with the organization's goals.

Review involvement examples

There are many ways in which human and cultural factors can be influenced to produce more positive behaviors in organizations.

Playful approaches to engaging staff include quizzes, security games, or brain teasers that employees can also take home. To make the participation more attractive, a contest with a prize can be added.

Another action is the security arena—an awareness "circuit training" out of the box. Participants learn about security topics such as password hacking, social media, or clear desk policy—at individual stations, where there is a short briefing about the topic, then a mini game to solve, where winning teams are identified and awarded.

One can also use security moderation cards that management can use in team meetings. For every team meeting, there can be one card with one topic to deal with. This is not very time-consuming and leverages the regularity of an existing team activity, rather than removing employees from their work.

Whenever there is a campaign designed to address security issues and raise awareness, it is always helpful to choose real employees as protagonists. Employees will experience greater engagement and pay more attention if their colleagues are involved in the campaign, socializing security and related concerns while recognizing the influence of peers within groups.

Human vulnerabilities in security systems[15]
All stakeholders—owners, employees, and customers—have security needs, but may not associate them with security, or express them in security terminology. But management and employees usually have a good understanding of the organization's key assets and processes, and linking security to this understanding helps develop security that fits with the business, and increases awareness and motivation. This is why a participatory approach to security analysis and design—involving stakeholders in the technical discussions and decision-making surrounding security design—is beneficial.

[15] "Human Vulnerabilities in Security Systems," Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P.; In Human Factors Working Group White Paper, Cyber Security KTN Human Factors White Paper, 2007

Another option is training with learning video clips, because they are not overwhelming to the participant. At the end of the video, it is possible to add a little quiz or question to encourage interaction.

Clear Desk audits are very popular measures—explicitly or covertly, such as part of an audit or penetration test. If a desk is clear, you could put a green card on it, otherwise, a red card, providing a hint that the solution of this card is hidden on the security intranet. This way you get people to talk to each other and promote interaction. The organization clearly has to decide whether to punish or engage with employees.

A new way of introducing security awareness is Edutainment. This can be in the form of a Lunch & Learn event that's combined with a live hacking event or play that deals with security issues. If employees attend, they will spread their new learned knowledge virally.

Another example of how to start an awareness campaign is to give security an identity in the organization. It can be a virtual identity, which serves as a middle-man between employees and security issues. Or a cartoon character can be developed and serve as a link. These identities should even have their own email address to encourage communication. It has to be clear and explicit that this campaign belongs to this company, using symbols and branding.

There are many creative and effective ways to involve employees in security issues, but the overarching recommendation is that every campaign be tailored to the needs of employees and created in a way that respects the individual, providing something useful. Content within each of these involvements can be crafted based on the outcomes of engagements with employees.

Consider these points

From this report, there are a number of key points for you to consider when developing or revisiting awareness campaigns:

1. CET cannot compensate for security policies and implementations that are impossible to comply with—removing impossible security tasks is essential security hygiene.

2. The purpose of security awareness is to achieve lasting behavioral change. A combination of CET activities can affect this change.

3. Before implementing any CET measures, each organization must identify areas of improvement and take baseline measurements. It is important to understand the current security culture before trying to create a new one.

4. Each security awareness campaign needs to be tailored, ongoing, and involving. Ideally employees will receive a skill set that helps them professionally and privately.

5. A balance must be made between prescriptiveness of policies and the practicality of enacting them. If there are too many policies, the cost of compliance can become too high and limit productivity and adaptability—policies must be workable, so consider where policies are rules and where they are guidelines.

6. Habit change requires effort and motivation from the individual and oversight from the organization. There is a personal cost to changing routine behaviors; so be sure to communicate a valid reason and the benefits of changing it—treat habit change as a value proposition, not a mandate. Behavior change is not a case of delivering more and more content to people, and should be target-specific content on different channels.

7. Intervention is not just about changing behavior, but also about how employees are involved in the process. A visible effort to engage with staff may be appreciated—design new things, try to get people involved, be brave. It ultimately relates to the purpose better and must identify with the company culture and goals.

8. It is necessary to understand cultural differences, character types, and the context, as they relate to individual capacity.

Make it relevant

By doing all of this, your organization can build an effective and sustainable IT security system and culture that cuts across processes, hierarchies, and roles. A clear view of the organization, its culture, and interdependencies means security awareness can be targeted to specific groups of employees, delivering a set of core and appropriate level of security skills relevant to your individual company.

About the authors

Marcus Beyer, Hewlett Packard Enterprise, senior awareness architect

Sarah Ahmed, Hewlett Packard Enterprise, security awareness consultant

Katja Doerlemann, Hewlett Packard Enterprise, security awareness consultant

Simon Arnell, Hewlett Packard Enterprise, chief technologist

Simon Parkin, UK Research Institute in Science of Cyber Security (RISCS), UCL, senior research associate

Prof. M. Angela Sasse, FREng, UK Research Institute in Science of Cyber Security (RISCS), UCL, director

Neil Passingham, Oxio, director

CESG
The Information Security Arm of GCHQ

RISCS
Research Institute in Science of Cyber Security

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-3090ENW, December 2015