Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours

M. Angela Sasse(✉), Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann

Human Centred Security, Ruhr University Bochum, Bochum, Germany
Martina.Sasse@ruhr-uni-bochum.de

Abstract. Most organisations are using online security awareness training and simulated phishing attacks to encourage their employees to behave securely. Buying off-the-shelf training packages and making it mandatory for all employees to complete them is easy, and satisfies most regulatory and audit requirements, but does not lead to secure behaviour becoming a routine. In this paper, we identify the additional steps employees must go through to develop secure routines, and the blockers that stop a new behaviour from becoming a routine. Our key message is: security awareness as we know it is only the first step; organisations who want employees have to do more to smooth the path: they have to ensure that secure behaviour is feasible, and support their staff through the stages of the *Security Behaviour Curve* – concordance, self-efficacy, and embedding – for secure behaviour to become a routine. We provide examples of those organisational activities, and specific recommendations to different organisational stakeholders.

Keywords: Security learning curve · Security awareness · Security training · IT-security for IT professionals · Organisational security · Human factors in IT security

1 Introduction

The vast majority of organisations in advanced economies buy some form of security awareness or security training for their employees. But despite the ubiquitous use commercial products, of there are doubts whether these are effective. In 2015, the UK Research Institute for Sociotechnical Cyber Security (RISCS) published a report that identified a fundamental problem with existing products: they raise awareness of IT security risks, and explain what employees should do and not do to be secure - but they do not support the adoption of those behaviours in everyday practice [9]. The authors proposed a 6-step process necessary for a secure behaviour to become an embedded routine, and identified a number of measures through which organisations could to support the transition to the secure behaviour at each stage.

S. Katsikas et al. (Eds.): ESORICS 2022 Workshops, LNCS 13785, pp. 248–265, 2023.
https://doi.org/10.1007/978-3-031-25460-4_14

To date, this report had little to no effect in practice – the global business of security awareness/training has grown into an even bigger, multi-billion $ a year industry. Yet, security researchers and practitioners find that employees are not following secure behaviours [2,3,18]. And yet, security and organisational decision-makers keep buying those awareness and training products, compel busy employees to spend time and attention on working through them every year, and somehow expect a different result – bringing to mind Einstein's definition of insanity.

In this paper we present a framework for breaking this cycle by supporting the adoption of secure routines. Beyond explaining security risks telling employees the do's and don'ts of IT security, organisations need to stop the execution of existing insecure behaviours, and embed new secure ones. This requires changes to artifacts and processes that employees deal with in their working environment. Over the past decade, behavioural scientists have been pointing out how environment can help or hinder important behavioural change - most notably. Michie et al.'s Behaviour Change Wheel [23]. Thaler and Sunstein's [30] famous nudge theory showed how policy makes can create choice architectures that encourage behaviour changes that ultimately benefit the individual. Both of these approaches have been enthusiastically seized on by security researchers - see [31] for an overview. Chater and Lowenstein [11], reviewing a broad range of nudge-based interventions come to the sobering conclusion that they have led rarely been successful - because they focused exclusively on trying to persuade individuals to change, while making little to no adjustments to system around them. That is also the case in IT security - an ENISA meta-review [12] of studies trying to link human characteristic or motivational factors to "good" security found no systematic link (except self-efficacy, see Sect. 2.)

In this paper, we bring insights from behaviour change literature together with specific literature on human behaviour in security ([7,19,27,31]), and spell out what organisations need to foster secure behaviours among their employees:

1. **Conduct a feasibility check: The most basic pre-condition is: never ask employees for a security behaviour unless you have checked it is actually possible to do in their work environment.** Employees can only adopt security behaviours that are feasible are in the context of their everyday work tasks. This may sound obvious, but most commercial products deliver general-purpose advice that has never been checked for relevance to, or feasibility in, the organisation. Some packages contain outdated recommendations that - for instance, they recommend long and complex passwords, and regularly changing them, when advice by relevant national authorities (e.g. NCSC) changed over 5 years ago [24]. Simply buying a generic security awareness package or simulated phishing product, just to tick a box saying *"yes, we provide security training"* is a clear sign an organisation did not really engage with security issues and how they might affect their business.
2. **Create secure routines:** Humans are efficient because everyday behaviours are embedded in **routines or habits**. About 80–90% of behaviour at work and in daily life is carried out in this mode. Kahnemann [17] labeled this *fast thinking*, as opposed to the *slow thinking* process we apply to novel and

infrequent tasks. In the latter mode, we apply our full attention to the task, but are considerably less efficient. Switching to the slow mode can occasionally may be viable, but telling employees to switch to the slow lane and ponder security implications of everything they do is not viable in busy production environments.

3. **Protect productivity:** Humans at work are focused on their *primary production tasks* – the security tasks employees have to carry out are *enabling* or *secondary tasks.* Any time spent on secondary tasks comes at the **expense of productivity** – and that includes security awareness, education and training measures. In almost any organisation, there is a limit to how much productivity can be sacrificed for security. Thus IT security measures need to be designed to be efficient in terms of time and attention, and with the participation of employees.
4. **Respect and engage employees:** Traditionally, employees have been cast in a passive compliance role when it comes to security; studies over the past decade have shown that **employee participation and agency** lead to better security behaviour and more effective protection.

Once an organisation has security made feasible, it may still find employees follow a number of insecure routines that need to be decommissioned and/or replaced by new, secure ones [13].

2 Enabling the Acquisition of Secure Behaviours

The *Awareness Maturity Curve* (Fig. 1) was originally developed by Beyer, Dörlemann and colleagues at HP Enterprise [9]. A notional rather than an operational concept, it illustrates that most organisations only provide resources on for motivating and informing employees about IT security behaviours, and then stop - and identifies the additional stages that would be required to embed new secure behaviours. The RISCS White Paper *Awareness is only the first step* [15] presented a further steps that need to be completed to embed *secure behaviour*, and pointed out that organisations did not consider or support these.

In a similar vein, Renaud et al. [28] argue that *usability is not enough*, and present a comprehensible model (Fig. 2) of requirements for the adoption of secure technology (in this case, E2EE).

In 2021 Hielscher et al. [16] presented the first version of the *Security Learning Curve* (Fig. 3) which incorporates recent scientific advances on individual learning and learning in organisations. We argue that those insights provide the "missing links" that organisations need to support to enable the adoption of secure behaviours among their employees. The bad news is that those steps require significantly more effort from organisations than what they do at the moment: buy standard materials from external vendors, deploy in fire-and-forget mode to satisfy regulatory or audit requirements (yes, our employees have been giving "awareness training"), then complain that employees are still not following the rules. The good news is that it is possible to embed secure behaviours and reduce the likelihood of breaches and the resulting cost. Most organisations

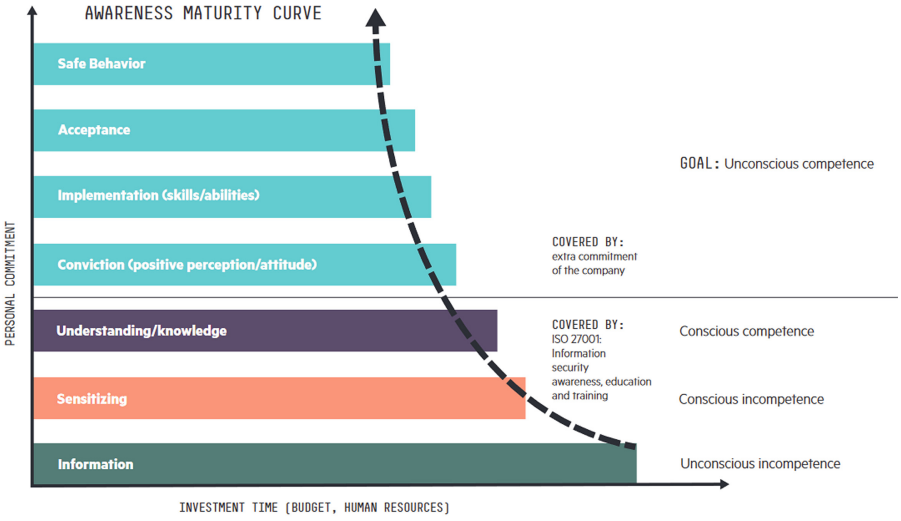

Fig. 1. The original Awareness Maturity Curve, presented in 2015 [9].

already practice a similar approach to safety since the late 80s, and organisational leaders often quote the phrase *"If you think safety is important, try an accident."* The same goes for IT security: *If you think supporting the embedding of secure routines is expensive, try a security breach.*

The Security Learning Curve consists of 9 stages people pass through to embed a new secure behaviour. Only 4 are covered by present mainstream awareness products – but that does not mean they are effective as mostly in form of standard materials that reflect requirements or recommendations of government agencies (e.g. Cyber Security Essentials in the UK, NIST recommendations in the US) or regulatory bodies (e.g. PCI-DSS for payment processors). Sometimes the awareness materials have been adapted to the risks relevant to the organisation, and/or the language it uses in other communications with employees. Fewer organisations then target the material according to the risks associated to the job role. Only a vanishingly small number of organisations bother to take stock of what individual employees already know and do when it comes to cyber security, and adapt their materials accordingly - thus wasting employees' time and goodwill on repeating what they already know. In this paper, however, we focus on the remaining steps, which are currently not supported. Before examining those steps in detail, it is worth pointing out that whilst the steps mirror a path to embedding behaviour, they do not always have to be completed in this order, but overlap or run in parallel.

As pointed out in Sect. 1, feasibility of the secure behaviour is a necessary pre-condition for its adoption. In the original *Awareness Maturity Curve*, this was mentioned in the text, but not represented in the curve itself - which in hindsight was a mistake. Research has shown that when employees don't follow

security policies, it is mostly because either they cannot do it [1], or because doing so would noticeably reduce their productivity [7], [19]. Parkin et al. [25] outlined an approach for tracking security workload in organisation, but virtually none keep track of their employees workload.[1]

Sensitising. This is *security awareness* in its classic sense: making employees aware of threats, and the risks and potential consequences for the organisation. Whilst many security awareness products - as well awareness campaigns by governments or law enforcement -explain specific attackers and specific forms of attack, most organisations need to do a better job at informing their employees about the specific risks the company faces, the consequences, and how employee behaviour can enable or prevent such attacks. Also, highlighting relevant risks to different groups of employees - rather than tell all employees about all IT security risks - helps employees to recognise their specific responsibilities, and motivate them to embark on the (always effortful process) of giving up a deeply embedded insecure routine.

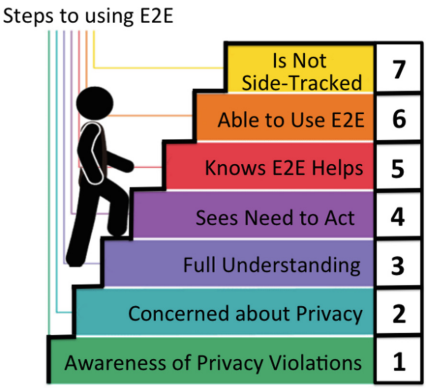

Fig. 2. Renaud et al. [28] argue that *usability is not enough* and present a model that shows additionally required steps.

Information. Once awareness of the risk has been raised, organisations need to specify the secure behaviour employees must follow to avoid/manage the risk *after*.

Understanding. There can also be benefits providing some background knowledge beyond the secure behaviour - for instance, explaining connections between risks. Systematically building up an understanding of threats and risks beyond

[1] Note that in the *Awareness Maturity Curve Information* comes before *Sensitising*. In the SLC we change the order as sensitising is a necessary pre-condition for rendering people amenable to change - and that is almost always by providing information about threats and consequences.

specific secure routines helps to build a broader understanding, and can enable employees to respond to novel, "not-yet trained for" risks.

Traditional approaches to security awareness, education and training stop here – they expect that once employees have understood the risks and know what to do to avoid them, they will change behaviour. But we know from research in behaviour change that good intentions are not enough. For a new behaviour to "stick", it has to be repeated over a period of roughly 28 days to become routine. The following 5 steps are elements that need to be in place to complete the *Security Learning Curve*:

Agree to changing behaviour: Concordance. There is a difference between employees agreeing that a secure behaviour is a "probably good idea", and actively making an effort to adopt it. Secure behaviour is currently mandated by security experts, and employees are expected to *"just do it."*. But change requires effort, people have many demands on time, and - if the behaviour has been mandated without consultation - many possible excuses for not even trying. The problem is illustrated by one of the classic lightbulb jokes *Question: "How many psychiatrists does it take to change a lightbulb?" Answer: "Only one – but the lightbulb really has to want to change."*[2]

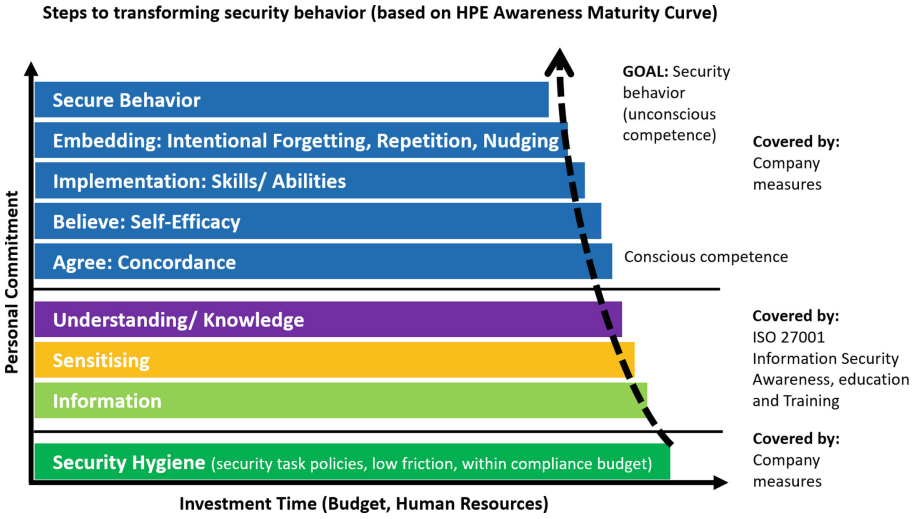

Fig. 3. The new *Security Learning Curve*, presented in 2021 by Hielscher et al. [16] that we extensively discuss in this paper.

The psychiatrist-lightbulb joke neatly conveys the central tenet of successful behaviour change: it requires positive intention and commitment from the

[2] In some organisations and under some circumstances it is possible to impose behaviours, but it is expensive because it requires constant monitoring and willingness to impose sanctions – such as firing employees who do not comply.

individual to make the change. In the medical sector, the approach has been adopted not only in mental health, but medicine taking [21]: *"Concordance is a new approach to the prescribing and taking of medicines. It is an agreement reached after negotiation between a patient and a healthcare professional that respects the beliefs and wishes of the patient in determining whether, when, and how medicines are to be taken."*

Applying the concept to IT security means that there needs to be a stage for employees to explicitly commit adopting the new behaviour. Most employees want to protect their organisations from harm, but they may have questions about the feasibility and effectiveness of the behaviour in the context of their own work-related goals and activities – so their needs to be an opportunity for clarification and negotiation. This means security behaviours cannot be mandated by experts without consultation. Ashenden and Lawrence [4] demonstrated the benefits of security experts explaining and negotiating the secure behaviours they want with employees, and the participatory security design case studies by Lizzie Coles-Kemp and her collaborators have shown [14] such engagement not only helps to get people "on-side", but can lead to security solutions that are more effective and less costly than ones experts had devised themselves.

Believe Behaviour is Possible: Self-efficacy. In a meta-review of studies trying to identify factors that influence cyber security behaviours, only one factor could be consistently linked to security behaviours: self-efficacy [12]. The concept was first described by Bandura et al. [5], who found that the belief in one's own abilities to do something successfully and is positively related to the implementation of a change in behaviour. Conversely, if employees have no confidence in their ability to perform a new behaviour, they are more likely not to try it in the first place. The execution of a new behaviour and the positive experience that they can do it should therefore be an essential part of IT security training. If, for example, employees have experienced in a role play that they can stop someone trying to sneak through an access control (tailgating) and deal with a confrontation that may result, they will be more willing to implement this behaviour in their daily work [6]. An individual's self-efficacy is influenced by four factors [5]:

Mastery Experience. An employee who successfully confronts someone tries to tailgate behind them is an example of positive mastery experience. Practising that behaviour in role-playing exercises, with feedback and coaching, can enhance employees' belief in their own ability. When encountering the threat in practice, they can refer back to similar scenario and recall how they acted. Direct experiences can have both positive and negative effects on self-efficacy expectations. Employees only have positive direct experiences if the action is their own and they consciously make their own decisions in this action. The belief in one's own abilities is thus strengthened by the fact that employees – since they act independently – get the feeling of having control over the situation. In the case of negative direct experiences, the feeling of loss of control and failure arises and employees begin to doubt their abilities. It is therefore important that in the case

of negative direct experiences, the other three factors are taken into account so that employees are not left alone with the negative experience.

Vicarious Experience. Vicarious experience means that when employees see, for example, a video of another person mastering a situation, they assess their own abilities similarly. One of the ways employees gain vicarious experience is through everyday encounters. In this context, team members and supervisors function as social role models and, in best case, as positive examples for their own actions. Depending on the degree of self-efficacy already present, it is more likely that views and behaviours gained through vicarious experience will be internalised. Another component that can play a role in vicarious experience is the trust relationship between the employee and the observed person. For example, if a very trusted colleague is observed making a mistake and is sanctioned, this can have a negative impact on the employee's self-efficacy expectation and thus on their future behaviour. Video material and working with personas are also approaches which let employees gain vicarious experiences.

Verbal Persuasion. Verbal persuasion can happen, for example, through feedback processes. If an employee receives positive feedback when completing tasks they will become convinced that they have or can develop the skills needed to complete the task successfully. Whether an employee can be convinced to trust in their own abilities also depends on the hierarchical relationship, but also the relationship of trust, between those who communicate. A hierarchical relationship alone is not enough to convince employees that they are up to the task.

Emotional and Physiological States. Companies should not trigger fear in their employees, but give them the feeling that they can contribute to IT security themselves. But how do conditions arise that inhibit behaviour, such as the fear of behaving incorrectly? Often it is physical reactions (such as stress, tension, heart palpitations) that are triggered by external input, such as instructions, tasks or spontaneous changes. The employee's brain may interpret these physical reactions in such a way that a reaction that is expressed in actual behaviour does not occur. Employees may avoid secure behaviour because they interpret a physical reaction as a warning signal. It is therefore important not to punish employees who are unsure what to do, or panic and make mistakes. Moreover, it is crucial to identify these warning signals and behaviour-inhibiting conditions in time so that insecurity cannot take hold. In practice, however, the opposite is usually observed: fear appeals are widely used in security awareness materials to in the mistaken belief that they motivate employees. But e-mails warning about the latest threats and the consequences of 'misconduct', without taking into account that employees also need to get the feeling that they can successfully protect themselves, can backfire. Direct and indirect threats of sanctions are also common, e.g. by sending individuals or teams to follow-up training or talks with superiors for poor performance in phishing simulations.

Applying the Four Factors to IT Security Behaviours. This approach shows that it is not factors internal to employees, but the context and the situational circumstances they experience that influence whether they try to adopt new secure behaviours. In the tailgating example, avoidance behaviour can have various causes that lead to employees unconsciously deciding against secure behaviour, and not intervening when they see an attack. Low self-efficacy expectations can often be traced back to negative direct experiences or experienced negative consequences through vicarious experiences. Negative feedback or one's own physical reactions to an attack situation can also be the reason.

In an organisational context these four factors are often closely linked: negative direct experiences can cause physical reactions, which in turn can cause negative feedback from the environment (directly from superiors or colleagues, indirectly via communication by e-mail from security staff or customers) - thus reinforcing avoidance behaviour. For a good implementation of IT security measures, it is necessary to strengthen self-efficacy not just in training, but the everyday work environment, by providing positive feedback when they apply the new behaviour, and support and re-assurance if they encounter difficulties (Fig. 4).

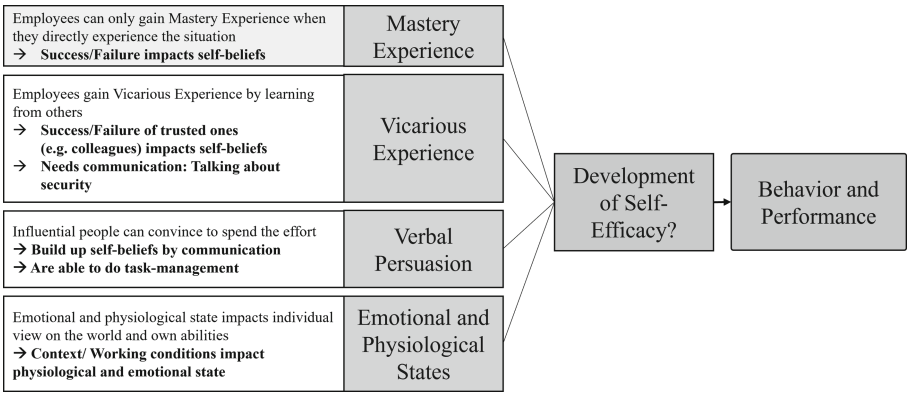

Fig. 4. Four factors influence self-efficacy.

Implementation. Once concordance and self-efficacy have been established, the next step is to embed the behaviour in the context of everyday activities. Key to achieving embedding is that a new secure behaviour cannot be embedded while the "old", insecure behaviour keeps being triggered. Established behaviour are deeply embedding in long-term memory, and triggered by cues, and then executed automatically. Every time this happens, the old behaviour is reinforced and embedded more deeply, making the embedding of the new behaviour impossible. Existing security awareness approaches implicitly suggest that once employees have received information about a secure behaviour, they just have to be motivated enough to change. This is not so: the organisation has to identify and remove the triggers of the "old behaviour from the tools, processes and environment".

Embedding. The new secure behaviour has to be repeated many times to become embedded. With every repetition, we move forward on the path to it becoming automatic, but every time the old, insecure behaviour is carried out, we go 3 steps back. Companies need to take active steps to decommission old behaviours, and remove the cues or triggers for them – a technique called Intentional Forgetting that has been successfully applied in the introduction of new safety procedures. In IT security, the need to *"take out the trash"* – removing obsolete rules and terminology, changing user interface design and processes as well as policies – is currently not understood.

Organisations can use tools to implement intentional forgetting and replace "old" insecure employee behaviours with new secure ones. First and foremost, the cues that trigger insecure behaviour – sensory, routine-related, and space and time-related stimuli – must be identified and removed. Hielscher et al. [16] provide examples of how to enable new secure behaviours by changing names for information objects and processes or re-designing desktop environments (e.g. a changed screen background/logon screen in the home office – a visual cue that is then linked to the need to connect to a VPN). Newly recruited employees can be trained in the secure behaviours, and be briefed to become "agents for change" who remind and support existing employees in their teams with the new behaviour. In organisations that have security champions [8], these can become forgetting agents who identify and eliminate triggers. The example of password managers shows that adoption becomes much easier if other applications and habits are changed at the same time. Therefore, it is recommended to combine the introduction of password managers with other changes in order to establish a link between the use of the password manager and other new cues. Nudges have been used in security to induce security behaviour security, with mixed results [31]. The SLC suggests that nudges will be ineffective if those behaviours are too effortful, or without concordance and self-efficacy being established. Nudging employees towards secure behaviours has been tried in IT security, but has neither long-term success nor is it ethically justifiable [29]. But at the embedding stage, nudges can help to remind employees that they have committed to adopt a new secure routine, and why.

Secure Behaviour. Secure behaviour becomes routine. This is the stage at which the organisation can consider using rewards for those who have managed the transition, and consider sanctions for those who won't. Organisations use psychological contracts to set expectations for employee behaviour in many areas – for instance, that bullying or harassment are unacceptable. Secure behaviours should also be seen as part of organisational citizenship. Embedding the steps of the SLC in an organisational change management process [20] helps to stage the adoption of secure routines and avoid conflicts with other organisational goals. However, due to the constantly changing threat landscape, more than routinely carried out behaviour is needed. Employees need *competence* to deal with unforeseen situations, in which routines are not sufficient, in a secure manner. We expand on this in the following.

3 Beyond Secure Routines: Building Competence for "Security Heroes"

Getting employees to develop secure habits it essential for making security efficient. Telling employees to "take 5" in the name of security every time they carry out a frequent task, such as opening an email, is unrealistic. 80–90% of human behaviour is carried out automatically, and demanding that employees stop this to take conscious cognitive decisions all the time ignores that individual and organisational productivity is built on routine.

Further, we cannot prepare employees for all possible risks – attackers innovate constantly and find new attack vectors. As soon as we have "trained" employees about an attack in an awareness campaign, attackers will have developed another way. As Janet Napolitano famously said, "Show me a 50-foot wall, and I'll show you a 51-foot ladder" (Janet Napolitano).

The true question here is: how can we prepare employees to recognise when a situation is novel or different, when they should switch from the "automatic" mode, examine the situation, and take a conscious decision? The awareness and training we provide to our employees must enable them to develop increasing maturity when it comes to security:

1. **Situational awareness:** Attackers often trigger highly learnt behaviours from employees by making a request look normal. Situational awareness can help employees to cope in new situations, and the decision not to follow established routines – if they feel secure enough to do so.
2. **Training for the things you don't normally do:** In situations of stress and uncertainty, we revert to highly learnt behaviours – this is where "training kicks in". That means that secure behaviours that we don't use all the time but need in emergencies – for instance disconnecting machines – need to be rehearsed. Link to business continuity.
3. **Agency and Active participation** in the development of security measures so they fit into the everyday work tasks and people feel included, strengthening their sense of belonging and shared responsibility.
4. **Strengthening qualities beyond security**, such as social skills, trust and cooperation, so that people feel secure to address errors, irregularities, or insecurities and know where to turn to.

Creating a work environment built on trust and cooperation, supporting employees in developing secure routines, and empowering them to confidently handle unexpected events is essential to make organisations resilient in a constantly changing threat landscape. Doing so will enable employees to become "Security Heroes" [26] in an organisation, instead of unsuccessfully trying to train them to become security xpert "mini-me"s.

However, the process does not stop here.

4 The Need for Evaluation and Continuous Improvement

Most organisations deploy IT security awareness and training in *"fire and forget"* mode - being able to tick the box "yes, we provide security awareness/training"

is the only goal. An Information Security Forum (ISF) report in 2014 found that less than half of all member companies that provided security awareness or training did evaluate whether it was effective. Organisations that do evaluation use quantitative measures that are easy to collect. In a more recent survey by Proofpoint 65% of respondents used completion of training as a measure of programme effectiveness, and 55% said they conducted a post-training poll or test.[3] Very few organisations check whether employees actually understood what the correct behaviour was, or whether they adopted it.

Evaluating how effective your awareness and training is, and identifying and improving the elements that are not, should be part and parcel of offering it - after all, security awareness and training that is not effective just wastes employees' time and reduces the organisation's productivity. Second, not collecting and acting on feedback from employees creates the impression among employees that security can't be that important – because if it was, the organisation would want to know.

4.1 "Well - I Wouldn't Start from Here"

If we ask general work-based training specialist what they think of current security awareness materials, they most likely quote the Irishmen asked for directions: *"Well - I wouldn't start from here"* – "here" being putting all employees through the same programme, irrespective of what they already know, or what risk and routines are relevant in their daily work activities.

The correct place knowledge quizzes on IT security is not *after* the training, but *before* employees are given any training at all. Evaluation needs a baseline measurement: find out what your employees already know about security, what they don't know - and then deliver targeted training. An added benefit of such a stock-taking exercise is that employees should be motivated to take securion topics they have been shown they don't know.

4.2 What is Success?

Having first evaluated the current state of security knowledge of employees and adapted the campaign accordingly, we need to ask: what is success? Is it that employees are able to answer questions in a test, however "gamified" and fun, what organisations want?

Only if we have clearly defined the desired outcome, can we develop metrics to measure whether the campaign was successful. As we have argued, it is neither enough to raise awareness nor to develop secure routines among employees, but we need to foster cooperation and resilience in regard to IT security and possible attacks in a continuous process that is never finished. To evaluate this,

[3] Information Security Forum (2014) From Promoting Awareness to Embedding Behavior. https://www.prlog.org/12319007-information-security-forum-embedding-positive-information-security-behaviors-in-employees-is-key.html.

an iterative mixed-methods approach is necessary – to evaluate the effectiveness of campaigns and measures in organisations, and to improve said measures perpetually within organisations as well as products by providers.

Simultaneously, the correct implementation of the measures should be evaluated.

In 2019, ENISA [12] proposed a PDCA-style framework[4] (Fig. 5) for designing interventions for human aspects of security that illustrates this process:

Fig. 5. ENISA's [12] PDCA-Framework for designing interventions for human aspects of cyber security.

4.3 How to Evaluate Security Awareness

Previously we discussed that employees should develop routines. Evaluation and continuous improvement of security awareness material and secure routines is important to support the behaviour change and the development of routines and secure behaviour. Implemented solutions to raise employees' security awareness need to be evaluated to see whether there are vulnerabilities in the implementation process or whether there is another solution that might fit more in the given context. Evaluation has the goal to make visible if awareness material or training is effective and if it fits working procedures or if it creates friction.

5 Conclusions and Recommendations

Security awareness and training today is a multi-billion $ industry that promises to fix "weak" employees and turn them into a "human firewall" through online security awareness courses, simulated phishing attacks, nudges and gamification. Employees may or may not learn something from these - we don't know because

[4] The Plan-Do-Check-Act Cycle, is an iterative design and management method used in business for the control and continual improvement of processes and products, and is suggested in the ISO 27000 family of standards as a way of monitoring and improving security interventions. It is also known as the *Deming Cycle* after the management scientist W. Edwards Deming, the father to Total Quality Management.

organisations do not conduct meaningful evaluation studies. But research on security behaviour in organisations has consistently shown that the secure behaviour organisations proscribe to their employees is rarely adopted in practice.

The current approach to security awareness and training stops with trying to motivate employees to be secure, and providing them with information in secure behaviour. The evidence from behavioural science, from Fogg [10] to Thaler and Sunstein [30] is very clear: to successfully adopt a new behaviour, it must (a) be easy enough to do perform, and (b) people have to want to change, and (c) the behaviour must be repeated many times until it becomes embedded and automatic. Single interventions - motivating employees with threat stories, or "nudging" them with constant reminders to "be secure" - do not lead to adoption of secure behaviours, nor do they engage employees in security and encourage them to step up and become security heroes when the organisation faces new threats.

IT security, including security awareness, is seen by most decision-makers as a technical problem that can be delegated to IT and security professionals. These experts, in turn, mostly have purely technical backgrounds - and not knowing any better, they try mandate secure behaviours and expect employees to do as they are told. With the introduction of the SLC, we propose rethinking this approach - you can engineer behaviour in organisations to a large extent, but it requires work changing the processes and technology to support the target behaviour. In the following, we summarise key takeaways for different stakeholders in organisations:

5.1 Board Members

1. *"Having a security awareness programme"* is a start, and may in some cases suffice to satisfy external compliance requirements. But to protect your organisation effectively, employees need to **practice secure behaviours**, not just know about them.
2. Buying a standard security awareness package may seem a cost-effective solution. But un-targeted standard packages are not effective in changing behaviours. At worst, they burn staff time and goodwill and create a negative attitude to security. Invest in measures that provide relevant, targeted knowledge and acquisition of secure routines.
3. Most organisations have existing expertise on how to encourage and support correct behaviours: boards should encourage joined-up thinking and collaboration to bring those resources to **building secure routines**.
4. Beware of simple indicators and easy metrics: quantitative indicators such as *training completion rates and percentages of staff (not) clicking on phishing emails* may seem like objective indicators of preparedness and progress. But they are not reliable indicators of whether staff practice secure behaviours on a day-to-day basis, or whether the organisation is secure. Boards need to encourage CISOs to **develop meaningful metrics** linked to key risks, and work on continuous improvement.

5.2 For Executives

1. *Security awareness* cannot fix impossible, time-consuming and cumbersome security measures. Executives need to help CISOs to **create low-friction solutions and integrate security into business processes**.
2. You need to **encourage staff to participate in security**: to ask questions when they don't understand security rules or reasons why they are needed, report errors or rules they cannot follow, and suggest solutions.
3. Executives need to **lead by example** on secure behaviours, and embed the topic in the discourse throughout. Many companies have workplace safety as a standing items in their team meetings, information security needs to be there, too.
4. Executives need to identify and **bring together different skills and capabilities** in the organisation to foster secure behaviour – e.g. corporate communications to devise unambiguous, consistent and positive messaging, human resources to incentivise secure behaviours via organisational citizenship contracts, assessment, and remuneration.

5.3 CISOs

1. *Security awareness* is not a fix for impossible, time-consuming and cumbersome security measures. You need to work with executives and employees to **find low-friction solutions**.
2. When it comes to security awareness, more is not better - less but relevant is. Don't try to turn employees into "mini-me" versions of yourself – focus on**routines they should follow** to do their job securely, and help them acquire those.
3. Changing behaviours is a serious undertaking that requires **long-term planning and resources**. You need support from executives and other organisational functions to transform insecure behaviours into secure routines.
4. To be productive and creative, **staff need to feel secure, connected, and believe in their future** in the organisation. This is why awareness methods that involve attacking staff and sowing distrust are counter-productive.

5.4 Security Specialists

1. You need to **be approachable and helpful**: employees should come to you when cannot follow a security behaviour, or when they have made mistakes.
2. Use **respectful language** – stop using phrases such as *weakest link*, and stop blaming users [22]. Refrain from using overly technical vocabulary and try to find a common language with other employees. Only then can they truly understand – and also pass on information to their colleagues.

5.5 Security Awareness Specialists

1. Your are not a megaphone for blasting out whatever security specialists want to tell employees. Your job is to act as a broker who helps to **identify which groups need what awareness and training, and how best to deliver it** – in the context of non-production demands that employees face.
2. **Constant evaluation** - what works, and what does not - is important. To do that, you need to identify meaningful metrics on whether secure behaviours are being followed, and whether staff are engaging with security - and low-effort ways of collecting those measurements.

Acknowledgements. We would like to thank the anonymous reviewers for their helpful suggestions for improving the our exposition of the SLC, and Prof. Simon Parkin (TU Delft) and Ceri Goncalves Jones (Lego Group) for their comments and suggestions on several earlier drafts. The work was supported by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany and (partly) also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
2. Alshaikh, M.: Developing cybersecurity culture to influence employee behavior: a practice perspective. Comput. Secur. **98**(November 2020) (2020)
3. Alshaikh, M., Naseer, H., Ahmad, A., Maynard, S.B.: Toward sustainable behaviour change: an approach for cyber security education training and awareness. In: Proceedings of the 27th European Conference on Information Systems (ECIS). ECIS, Stockholm & Uppsala, Sweden (2019)
4. Ashenden, D., Lawrence, D.: Security dialogues: building better relationships between security and business. IEEE Secur. Privacy **14**(3), 82–87 (2016). https://doi.org/10.1109/MSP.2016.57
5. Bandura, A., Adams, N.E.: Analysis of self-efficacy theory of behavioral change. Cogn. Ther. Res. **1**(4), 287–310 (1977)
6. Beautement, A., Becker, I., Parkin, S., Krol, K., Sasse, A.: Productive security: a scalable methodology for analysing employee security behaviours. In: Proceedings of SOUPS 2016, Twelfth Symposium on Usable Privacy and Security, pp. 253–270. USENIX Association, Berkeley (2016). https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-beautement.pdf
7. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 New Security Paradigms Workshop, pp. 47–58 (2008)
8. Becker, I., Parkin, S., Sasse, M.A.: Finding security champions in blends of organisational culture. In: Acar, Y., Fahl, S. (eds.) Proceedings 2nd European Workshop on Usable Security. Internet Society, Reston (2017). https://doi.org/10.14722/eurousec.2017.23007
9. Beyer, M., et al.: HP enterprise - awareness is only the first step: a framework for progressive engagement of staff in cyber security (2015). https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

10. Fogg, B.J.: Tiny Habits: The Small Changes that Change Everything. Houghton Mifflin Harcourt (2019)
11. Chater, N., Loewenstein, G.: The i-Frame and the s-Frame: how focusing on individual-level solutions has led behavioral public policy astray (2022). https://ssrn.com/abstract=4046264
12. ENISA-European Union Agency for Network and Information Security: Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity (2019). https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity
13. Heath, C., Heath, D.: Switch: How to Change Things When Change is Hard, 1st. edn. Broadway Books, New York (2010)
14. Heath, C.P., Hall, P.A., Coles-Kemp, L.: Holding on to dissensus: participatory interactions in security design. Strateg. Des. Res. J. **11**(2), 65–78 (2018)
15. Hewlett Packard: Awareness is only the first step: new white paper from RISCs, HPE and NCSC urges organisations to engage employees in order to improve cyber security
16. Hielscher, J., Kluge, A., Menges, U., Sasse, M.A.: "Taking out the Trash": why security behavior change requires intentional forgetting. In: New Security Paradigms Workshop, pp. 108–122. ACM, New York (2021). https://doi.org/10.1145/3498891.3498902
17. Kahneman, D.: Thinking, Fast and Slow. Macmillan, New York (2011)
18. KasperskyDaily: The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within (2017). https://www.kaspersky.com/blog/the-human-factor-in-it-security/
19. Kirlappos, I., Parkin, S., Sasse, M.A.: "shadow security" as a tool for the learning organization. ACM SIGCAS Comput. Soc. **45**(1), 29–37 (2015)
20. Kotter, J.P.: Leading Change: Wie Sie Ihr Unternehmen in acht Schritten erfolgreich verändern. Verlag Franz Vahlen, München (2011)
21. Marinker, M., et al.: From compliance to concordance: achieving shared goals in medicine taking. Royal Pharmaceutical Society, in partnership with Merck Sharp & Dohme (1997)
22. Menges, U., Hielscher, J., Buckmann, A., Kluge, A., Sasse, M.A., Verret, I.: Why IT security needs therapy. In: Computer Security. ESORICS 2021 International Workshops (2022). https://doi.org/10.1007/978-3-030-95484-0
23. Michie, S., van Stralen, M., West, R.: The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implement. Sci. **6**(42) (2011)
24. National Cyber Security Center: Password administration for system owners. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
25. Parkin, S., van Moorsel, A., Inglesant, P., Sasse, M.A.: A stealth approach to usable security: helping it security managers to identify workable security solutions. In: Proceedings of the 2010 New Security Paradigms Workshop. NSPW 2010, pp. 33–50. Association for Computing Machinery, New York (2010). https://doi.org/10.1145/1900546.1900553
26. Pfleeger, S.L., Sasse, M.A., Furnham, A.: From weakest link to security hero: transforming staff security behavior. J. Homel. Secur. Emerg. Manag. **11**(4), 489–510 (2014)
27. Reeder, R.W., Ion, I., Consolvo, S.: 152 simple steps to stay safe online: security advice for non-tech-savvy users, vol. 15, pp. 55–64. IEE (2017)

28. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't Jane protect her privacy? In: De Cristofaro, E., Murdoch, S.J. (eds.) PETS 2014. LNCS, vol. 8555, pp. 244–262. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08506-7_13
29. Renaud, K., Zimmermann, V.: Ethical guidelines for nudging in information security & privacy. Int. J. Hum. Comput. Stud. **120**, 22–35 (2018). https://doi.org/10.1016/j.ijhcs.2018.05.011
30. Thaler, R.H., Sunstein, C.R.: Nudge. The Final Edition, [Revised edition, 2021] edn. Penguin Books, Yale University Press (2021)
31. Zimmermann, V., Renaud, K.: The nudge puzzle: matching nudge interventions to cybersecurity decisions. ACM Trans. Comput.-Hum. Interact. **28**(1), 7:1–7:45 (2021). https://doi.org/10.1145/3429888