This is a peer-reviewed, author's accepted manuscript of the following conference output:
Renaud, K., & Warkentin, M. (2017). Using intervention mapping to breach the cyber-defense deficit.
Paper presented at 12th Annual Symposium on Information Security, Albany, United States.

Using Intervention Mapping to Breach the Cyber-Defense Deficit

Karen Renaud[1,2,3]
[1]School of Computing Science
University of Glasgow
Glasgow, G12 8RZ, United Kingdom
[2]University of South Africa, Pretoria, South Africa
Email: karen.renaud@glasgow.ac.uk

Merrill Warkentin[3]
[3]Department of Management & Information Systems
Mississippi State University
Mississippi State, MS 39759, USA
Email: mwarkentin@acm.org

***Abstract*—It sometimes seems that every IT user is a combatant, engaged in a battle with multitudes of hackers across the globe. This battle is unevenly biased in favor of the hackers, because people routinely act in ways that open doors for hackers, thereby enabling their nefarious activities. If current approaches to raising security awareness were working the hackers would not be having as much success in attacking systems. It is time to reconsider how we design, formulate and deliver security awareness training. In this paper we propose using a technique borrowed from the health arena, "Intervention Mapping," to target security awareness training more effectively. We detail the different phases of the methodology and give an example to show how it was applied to an SME. The purpose of this paper is to open a discourse in the community about how we can arrive at more effective awareness-raising endeavors.**

I. Introduction

The era of ubiquitous connectivity has ushered in a brave new world where people can access information about any topic under the sun, and contact others at any location across the globe within seconds. The speed at which this new functionality has become available has left something of a void with respect to security. Many computer owners do not know how to secure their own, or their organization's, information. Even if they do know, they sometimes do not apply this knowledge effectively [58]. The reality is that many computer users are not resilient enough to spot or resist attacks, a situation we will refer to as a *cyber-defense deficit*.

This deficit has, unfortunately, been exploited by unscrupulous hackers, as evidenced by multiple attacks carried out daily on the unwitting and unwary across the globe. Organizations are clearly aware of the cyber-defense deficit, even if they don't refer to it by this name. The Ernst and Young 2016/17 Global Security Survey [36] reports that 73% of organizations are concerned about a poor level of awareness amongst their employees. The ISO 17799 standard [52] flags security education as one of the key aspects to be addressed to maximize the security of an organization's systems and information. Failure to address the cyber-defense deficit will inevitably lead to fiduciary loss and reputational damage [18], [57], [50].

Organizations tend to attribute the weakness in their defenses to a *knowledge gap* [4], [49]. The obvious way to bridge a gap is to deliver training to ensure that the requisite knowledge is provided [14], [92]. However, training, while essential, is not guaranteed to be 100% efficacious.

There are three dimensions that influence the effectiveness of security awareness training:

1) **Design:** deciding which (in)security issues to address,
2) **Formulate:** formulating the training: deciding how to frame and present the material, and
3) **Deliver:** deciding on a delivery mechanism.

There is surprisingly little agreement about the first aspect, as Section II-A will show. With respect to the third, there is little to quibble about — this often has more to do with budgetary and resource constraints within organizations than anything else. On the other hand, there is a uniformity with respect to the second (Section II-B) that might be contributing to the existence and intractability of the cyber-defense deficit (Section II-D). As a community, we need to seek out and design more effective awareness-raising formulations.

In this paper we propose a new methodology for maximizing the effectiveness of security awareness training (Section III), focusing here specifically on formulating the delivery of the material. Sections IV and V detail firstly applications of intervention mapping in other areas, then an information security application for an SME. Section VI reflects on the applicability of the new approach and Section VII concludes.

II. Related Research

A. Designing Training

Those designing security training within organizations often find it difficult to know which particular areas to include in the training. The employees attending the training generally have urgent tasks to return to, and it is easy to bore them or lose their attention if the training continues for too long. The person formulating the training is thus left with the task of choosing the most important topics to present. Essentially, they have to strike a balance between comprehensiveness and efficiency.

The ISO 17799 standard [52] does not provide much guidance with respect to what particular kinds of training ought to be delivered. They talk about addressing "*security requirements, responsibilities and business controls and the*

correct use of information." The generic nature of this list is perhaps due to the age of the standard and the speed with which attack vectors are changing and developing. Other publications also speak about security awareness in general terms, not being too specific about what ought to be included [80], [54]. It is probably unrealistic to expect any public body to be specific about what ought to be included in security awareness training, because experts agree that training should be tailored to the needs of the particular organization [34].

A number of academics are actively engaged in security awareness research, and attempt to guide awareness endeavors [23], [24], [55], [100]. For example, Vroom and Von Solms [100] make the case for security training and propose training on two fronts: (1) general practices, and (2) role-specific security. They then review the components of each of those, but do not explain how they decided to choose the particular components to include in the two broad categories. NIST [101] provides a list of topics to be covered, as do [66], [8]. Its lists are comprehensive, but are out of date now because of the speed of change in the cyber threat field. The more sedate march of research publication probably condemns them to being out of date as soon as they appear.

B. Formulating the Message

Having decided on topics to include in training, those delivering awareness training then have to formulate the training so as to deliver the material in the most effective way.

Ferrara [39] poses commandments of security awareness training, including the follows (1) serve small bites, (2) reinforce lessons, (3) train in context, (4) vary the message, (5) give immediate feedback, (6) tell a story, (7) make them think, (8) let them set the pace, (9) Offer conceptual and procedural knowledge.

Valentine [96] also advocates making training meaningful and advises making the awareness training scenario-based. He argues for a data-focused approach, moving away from a "Security Basics" model to offer specialized training that meets the organization's needs. He says training should aim to help end users to understand attack vectors and to explain how to respond if they feel they are being targeted by a hacker.

Albrechtsen and Hovden [5] also found that a participative approach was more likely to deliver behavioral change than traditional delivery of material via presentations, posters and emails.

These are all excellent guidelines for pure knowledge transfer, following sound educational principles [27]. Yet they stop short of explaining how to counter existing biases people might have [37], or how to counteract change resistance [61].

C. Delivering the Training

Awareness training can happen either before, during or after people carry out security-related actions.

"Before" training can be delivered in a number of ways. The most time consuming of these is face-to-face training. It does have some undeniable benefits. Having a trainer there in person affords trainees the opportunity to ask questions and to establish a connection with the instructor, which might ease subsequent interactions when they have follow-up queries.

A cheaper alternative is the use of web-based modules [44], with quizzes at the end to ensure that people are paying attention to the content. Shaw *et al.* [87] report that online training can be even better than face face training if the media is rich enough. However, this kind of training can only be applied to a small number of contexts, where it can indeed be very helpful [82]. It is expensive to develop, though, especially if tailored to a particular organization's needs.

A very poor and ineffective delivery mechanism is the use of paper-based handouts, often provided to new staff on the day they commence employment. Companies usually require employees to sign an undertaking that they have read the handouts. This gives an illusion that training has been delivered but does not actually ensure that the new employees understand the security culture of the organization [86] or have the efficacy to apply required security procedures.

"During" training is delivered as and when people are carrying out an action. For example, by providing dynamic strength feedback as and when passwords are provided [20], [31]. Other examples are the use of pop-ups and warnings as and when people carry out security-related actions [3]. There is little agreement, at present, as to the impact of these kinds of measures, with some researchers reporting positive effects [95] and others finding no impact at all [98], [88].

"After" training is delivered post-behavior. A number of researchers [53], [68], [91], [29] exploit something they call a *teachable moment* to teach people not to fall for Phishing messages. The organization sends fake Phishing messages to employees. If they fall for the Phish they are directed to a website explaining what they did wrong. It is particularly applicable to Phishing but not perhaps as easily applied to other contexts. These kinds of exercises are becoming popular in industry [38], [79]. This training is expensive, and could be considered unethical because it involves the use of deception.

The training we are focusing on in this paper is the "before" variety, perhaps more of a pure awareness approach than the "during" and "after" approaches, which could be considered to be *nudges* and *teaching-moment* approaches, respectively, as opposed to pure awareness training.

D. Behavioral Approach

Reports of successful hacks appear daily [33], [85], [78], [59]. Many attacks succeed because the hackers manage to dupe people into following a link in a Phishing email, or trick them into installing malware, or because they generally do something inadvisable, thereby allowing the hackers to gain access to an organization's systems. This still happens despite the huge efforts that go into security awareness training.

The latest wave of ransomware attacks attest to the fact that awareness efforts are not yet making their mark. It is time to find new ways of reducing the cyber-defense deficit and making employees more resilient. While current awareness-raising efforts do deliver some benefit [35], [67], a pure knowledge and/or skill dissemination approach is insufficient.

One of the reasons might be that organizations are unrealistic about what people will do with the information the awareness-raising training delivers. Many approaches assume that people simply need the requisite knowledge: that the knowledge gap needs to be bridged in order to improve resilience. The core assumption is that, having been apprised of the correct actions to take, employees will proceed to act as required.

For example, Furnell and Clarke [43] say *"the fact that incidents remain all too frequent is indicative of users not having understood their part in the security culture"* (p. 70). Yet knowledge, on its own, does not guarantee compliance or behavior change [6], [9].

Other authors model compliance using rationality-based models [51], [84] and also assume that people will maximize utility when making security decisions. Recent publications question the assumption of rationality, at least in terms of security behaviors [46]. Moreover, other fields have reported that knowledge, by itself, has little impact on behavior [40], [47], [58]. In particular, Pooley and O'Conner explain that attitudes, emotions and beliefs have to be acknowledged and targetted too [81].

Hence it becomes important to present awareness training in such a way that acknowledges that it needs to be more than a knowledge-transfer exercise. It should present the information as effectively as possible. By "effective" we mean delivering the information in such a way as to get past people's biases and resistance so that they accept and implement the practices the training is advocating. In essence, the training has to be informed by behavioral science research to maximize effectiveness.

The need to acknowledge and design awareness training with full cognisance of the behavioral aspects thereof is an issue that a number of researchers have highlighted [41], [89], [21], [83], [94], [25]. They stop short of proposing how this ought to be done though, something we address in the following section.

E. Summary

In conclusion, we need to move beyond the concept of a pure *knowledge* gap. To consider human behavior to be entirely predicated on availability of knowledge is to ignore "*the rich mixture of cultural practices, social interactions, and human feelings that influence the behavior of individuals, social groups and institutions*" [90, p. 2]. A more realistic *knowledge & behavioral gap* needs to be acknowledged if we are going to address the cyber-defense deficit.

III. Intervention Mapping

To address the *knowledge & behavioral gap* we have to acknowledge and design to accommodate the underlying behavioral *antecedents* of insecure behaviors. The training should be tailored specifically to ameliorate the behavioral determinants. Bridging the knowledge gap, on its own, is clearly not going to guarantee a change in behaviors unless the delivery mechanism also addresses the behavioral antecedents.

One way of looking at security awareness training is that we are essentially formulating an intervention to change behavior. In so doing we grapple with issues similar to those experienced by health practitioners. They, too, confront unhealthy behaviors that persist in the face of strong evidence related to their harmful consequences.

Information security researchers often benefit from the findings and practices of older, more established, disciplines. Health researchers propose and utilize an approach called *intervention mapping* [76] to formulate more effective ways of persuading people to change their health-related behaviors. We believe this approach is worth trialling in the information security domain too.

A number of different approaches to intervention mapping were consulted in order to tailor the process to the information security context [11], [62], [63], [64], [26], [7], [97]. Michie and Johnston [76] propose a two step process, whereas Bartholomew and Mullen [11] propose a four step process. Kok *et al.* [62] augments the previous plan with two extra steps, a plan for implementation and evaluation. The latter approach has been embraced by other researchers [64], [26], [7]. Table I presents an overview of the different proposed approaches.

Stage	[11]	[62], [64], [26], [7]	[76]
Problem behaviors	(Graphical)✓	✓	
Desired behaviors	(Graphical)✓		
Mechanisms of Change	✓	✓	✓
Map Interventions to Mechanisms of Change	✓	✓	✓
Implementation & Evaluation Plan		✓	

TABLE I
Intervention Mapping Stages

A. Applying Intervention Mapping to Information Security Awareness Raising

Figure 1 is a graphical depiction of the process we have derived from the approaches summarized in Table I to tailor it to the information security context. We describe the phases below.

1. Enumerate Insecurities Organizations identify the security issues they are experiencing that are related to employee behaviors. The activity can be described as a mapping from: `Insecurity` → `Problem Behaviors`

2. Identify Underlying Problem behavior The security issue is mapped to a particular human behavior that needs to be nudged in a positive direction. The activity can be described as a mapping from: `Security Issues` → `Problem Behaviors`

3. Map Antecedents of Behaviors The antecedent of the problem behavior is identified using two sources. The first, and most important, is to speak to the people who will receive the training and to ask them about the problems they face with

respect to the problem behavior. This should help us to identify organization-specific barriers. The second source is the research literature. The activity can be described as a mapping from: `Problem Behaviors` → `Antecedents`.

4. Identify Behavioral Change Mechanism The antecedent is mapped directly to Mechanisms for behavioral Change. The activity can be described as a mapping from: `Antecedent` → `Change Mechanism`

5. Identify Desired behavior The problem behavior is mapped directly to changed (desired) behaviors. The activity can be described as a mapping from: `Problem Behaviors` → `Desired Behaviors`

6. Design Interventions Interventions are proposed that are formulated to change behaviors, in a way that exploits known change mechanisms. The activity can be described as a mapping from: `Desired behavior + Change Mechanism` → `Interventions` and is essentially the deliverable of this process: the security awareness training

B. Behavioral Change

It is extremely hard to change behavior [22], [69]. A change to complex behaviors, like most security behaviors, necessarily requires an understanding of the barriers that exist for the activity to change. Because of this, information campaigns are unlikely to bring about any meaningful change unless they address the barriers [75]. Naïve carrot or stick approaches are also unlikely to make an impact and may indeed lead to unintended negative side effects [19], [70], [71].

The field of behavioral economics has led to a popularisation of techniques for steering people towards wiser choices [93], [48]. The psychology literature also documents a range of phenomena where people's behavior can be changed by surprisingly small and inexpensive interventions [12], [28]. A comprehensive discussion of the range of techniques is infeasible here, but we can mention one or two examples of techniques that seem particularly applicable in this context.

One strong effect is that humans are loss averse and prefer maintaining the status quo i.e their existing behavior. If we market a non-change as a loss this might make them consider switching [56], [16].

Another example is that when a sense of urgency is invoked people do not think decisions through as clearly [30]. This propensity is exploited by Phishers, but we can also exploit this effect by eliciting a sense of urgency when we market a behavioral change.

However, the reality is that if we want to change behaviors we ought to focus first on identifying barriers to change [74]. Having identified these, the best way to change behavior is to give people the resources to overcome said barriers.

One of the most prevalent barriers is that people lack efficacy to make and sustain a new behavior. It is of utmost importance, when we "sell" a new security behavior, that we ensure that people can perform the behavior well enough for them to experience a feeling of self efficacy in so doing [10].

C. Example

To explain how this approach would work, consider the following example:

1. Insecurity: The organization is concerned about hackers being able to gain access to their systems by guessing passwords.

2. Underlying Problem Behavior Weak password choice by employees

3. Antecedents of Behaviors: This is a hypothetical example so we cannot consult actual employees. However, based on the extensive literature on this subject, we can pinpoint the antecedents with some confidence. The antecedents are twofold. The first is that the organization forces people to change passwords monthly, meaning that password strength effectively reduces each month. The second antecedent is well known: human memory is limited and fallible. People are humanly unable to memorize multiple strong passwords. They know they will forget their passwords and be locked out of their accounts so they choose passwords that are easier to remember, and probably "weak" [1].

4. Behavioral Change Mechanism: Telling people to choose stronger passwords is unlikely to work nor will explaining what strong passwords look like. They have probably heard it all before. Unless we can persuade the IT department that their password change policy is actually misguided [15], [77], we have to identify a mechanism that ameliorates the antecedent: the memory issue. This is the barrier that no amount of admonition will eradicate, and until it is dealt with it is unlikely that people will improve their password choices. One way of removing the barrier is to promote the use of password managers. We could ask the organization's IT department to approve one for use in the organization. This effectively removes the behavioral antecedent.

5. Desired behavior: People choosing stronger passwords.

6. Intervention: Introduce an approved password manager. Sell it as a labor saving tool. Show people how it works and help them to install and use it. Offer short term assistance and support for installation and use. Offering assistance in the short term introduces a sense of urgency and will make them less likely to put off installing the tool. Activate loss aversion in two ways: (1) Offer them the tool cost free for a limited period, (2) offer technical assistance in the short term to help them with initial hurdles.

D. Summary

The usual awareness training, where a pure knowledge gap is assumed, will provide explanations of how to choose strong passwords. The trainer might also explain the consequences of weak passwords. This does not remove the barriers: it does not address the antecedents of the insecure behavior. So, while it might address the behavioral gap, it fails to effect a widespread change across the organization.

The Intervention Mapping approach proposes bringing some rigor into security awareness training. If this process is followed we ensure that (1) the actual problem behavior is targeted, (2) an intervention focuses on moving the employee

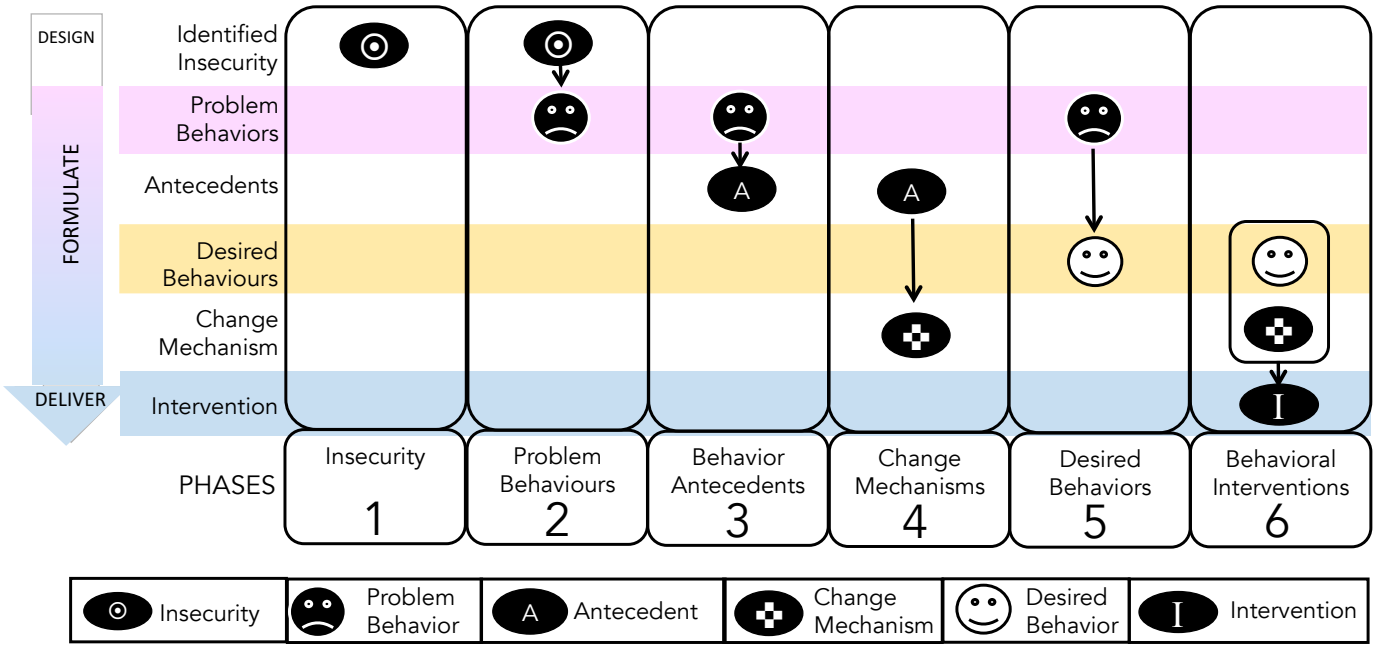

Fig. 1. Research Phases

towards an identified and articulated desired behavior, (3) the barriers to the desired behavior are acknowledged, and (4) formulation is informed by the insights from behavioral science research.

Any behavioral change intervention has to acknowledge the complexity and intractability of human behavior. With this approach we propose maximizing the effectiveness of interventions, even while we accept that there is no perfect mechanism to effect reliable and universal change.

IV. Applications in Other Disciplines

Kok *et al.* [65] provide an excellent review of a number of applications of intervention mapping. We mention three here.

Van Oostrom *et al.* [97] describe a successul application of intervention mapping in order to address the problems related to employees with stress-related mental disorders. The authors explain that, before the intervention, there had been no uniformity in applying work adaptation for employees returning to work after stress-related absences. In reflecting on the success of their intervention, they considered the involvement of various stakeholders throughout the process to be key. They also consider the fact that the approach closes the gap between scientific evidence and daily practice to be a particular strength, which makes it particularly helpful in addressing human-related issues.

Brug *et al.* [17] propose an intervention mapping approach to improving nutrition and physical activity. They point out that without this kind of approach, it is all too easy to apply interventions that have not been proven to be efficacious: they "lack a strong empirical foundation." They urge practitioners to use intervention mapping to ensure that genuine theories are used to promote nutrition and physical activity behavior change, rather than continuing with traditional approaches.

McEachen *et al.* [72] applied intervention mapping to help employees to be more active. They considered the methodology useful in informing the development of a theory-based intervention. A subsequent paper reported on the outcome of their intervention [73]. They report mixed results. Their intervention did not increase physical activity but it did significantly reduce systolic blood pressure resting heart rate compared to control. This suggests that the approach probably needs refining, and evidence from applications thereof can be used to feed into this refinement and improvement process.

V. Application of Intervention Mapping in Information Security

We carried out a intervention mapping investigation to help a local SME in Mississippi to target insecure employee behaviors. The investigation proceeded as follows:

Identify Insecurities:

An interview with the Information Security Officer revealed that she considered the main problems to be Phishing and Vishing messages, weak passwords, and insecure management of USB drives of unknown provenance.

Problem Behaviors:

The particular behaviors were (1) clicking on links in emails, opening email attachments, (2) using weak passwords and (3) trusting USB drives.

Antecedents:

We published an anonymous survey and asked people about the barriers that got in the way of their behaving securely with respect to the above-mentioned behaviors.

Phishing messages: Barriers fell into three groups: (1) those with a blame-worthy dimension (laziness, gullibility); (2) those attributed to an understandable human-related fallibility (not paying attention, not being careful enough, dealing with emails in haste or when fatigued, heavy workload) and (3) those where the respondent demonstrated empathy for the person who fell for the Phish (they were deceived, the email was expected or appeared to be from a known respondent, the email induced a fear response, they were curious).

Vishing messages: the respondents were not as judgemental in their responses here. Most suggested that people who fell for these were probably deceived because the caller had personal information about them, or because they felt they could trust a person who took the trouble to phone them. Some felt that there was a need to raise awareness to prevent people being deceived.

Choosing strong passwords: Some blame-worthy reasons, such as laziness and stupidity, were mentioned. However, most respondents pointed to the fact that people have too many passwords and simply cannot remember them all. A prior forgetting experience was deemed likely to change password behavior for the worse because the person did not want to repeat the experience.

Plugging in USB drives: Here three main explanations were mentioned: (1) curiosity, (2) an intention to return the drive to its rightful owner, and (3) people wanting to keep the drive for their own use. Only two cited ignorance of the company's policy in this respect.

Desired Behaviors:

The desired behaviors are for people to (1) detect Phishing and Vishing messages, (2) be wary of unknown USB drives, and (3) choose stronger passwords.

Change Mechanisms:

It is clear from the previous section that training and awareness drives are unlikely to make much of a difference. Many of the barriers are related to human nature, which is not changed by training. The responses with blame-worthy undertones are unhelpful. Pointing fingers merely makes people defensive: it does not lead to changed behaviors. Hence we identify more creative interventions that are designed specifically to remove the genuine barriers identified in the survey.

Interventions:

Resisting Phishing & Vishing: In this case an ounce of prevention is better than a pound of cure. People who are deceived do not deliberately fall for the lure. Improving awareness, while essential, is insufficient. Moreover, Phishing is an issue that organizations across the globe grapple with. There is no simple intervention that will prevent all Phishing attacks from succeeding. Three interventions are thus suggested:

(1) Regular awareness drives ought to be conducted — in the long run this is probably the best defense.

(2) It seems worth attempting to change the culture of dealing with emails after hours, or when fatigued. In France, for example, it is against the law for employees to deal with email after hours[1]. This ensures that people take sufficient time away from email to rest, and makes it more likely that they will be able to pay more attention to individual emails.

(3) The use of technical measures can bolster security. As soon as a Phish attack is identified a block should be put on that site so that any subsequent clicks by employees are blocked.

Choosing stronger passwords: Because the primary barrier is the limit of human memory and difficulty in coping with too many passwords, it is pointless to keep "educating" people about the need for stronger passwords. This does not remove the barriers and will fail to make any difference. The intervention has to address the barrier. The best way to do this is to promote the use of a password manager, as suggested in the previous section. The company could investigate these and assist employees with installation and initial adoption. This effectively neutralizes the memorability issue and there is no longer any barrier to strong passwords.

Not plugging in USB drives: The reasons cited here will not be changed by warning people about the potential consequences of this behavior. One cannot deactivate helpfulness, avarice or curiosity with admonitions.

One possible way to protect the company's systems is to provide a safe place for people to look at a USB they discover. One way would be to make available a basic computer that is not connected to the Internet or to the company network (with no access password). This computer should be available in a public place such as a common room; with a read-only hard drive, and be configured to scan any USB that is plugged in. People could plug in the hard drive and ascertain who the owner is, in order to return it. They could also reformat it if they want to keep it for themselves. If it does contain malware the scanner ought to be able to detect this, and the drive can be reformatted automatically. Now, all that has to be done is for people to be told to test any drives they find on this machine, rather than on their own. Offering people a safe way of satisfying their curiosity, avarice and desire to be helpful is much cheaper than dealing with the consequences of malware inadvertently being installed on the company's systems.

VI. Reflection

There is a school of thought that says we cannot train users to be secure and that security ought to be addressed by technical measures: that we ought to quit trying to get end-users to behave more securely [2], [13]. These authors have also alluded to the futility of security awareness training, arguing for a purely technically-focused approach to cyber defense.

[1] http://fortune.com/2017/01/01/french-right-to-disconnect-law/

Discarding training altogether is not an option for organizations, at least not those in developed countries. These organizations undergo yearly mandated security audits and have to show that they have security policies and also that they deliver regular security awareness training to apprise employees of correct security behaviors. Training is generally considered to be indispensable but we agree with [2], [13] that technical measures ought to be as sophisticated as possible so that the burden on the end user can be minimized.

The other drastic option is to avoid the use of computers altogether. After the NSA leaks it was reported that the Russian Intelligence service was switching to the use of typewriters [32]. After a recent hotel ransomware attack, Ghosal reports that the hotels in question are contemplating returning to traditional locks with hardware keys [45]. It is hard to imagine that many organizations have the flexibility or resources to abandon their IT systems altogether so this, too, is not really a feasible option.

Given that these two extreme options are unlikely to be feasible, what we should do, as some researchers have proposed, is to combine approaches, addressing both technical, governance and user aspects of security [99]. Khonji *et al.* [60] suggest a two-pronged approach, as do [23]. The first prong is user training, and the second technical measures such as automated detection. The latter includes blacklists, machine learning and visual similarity detection. Frauenstein and Von Solms [42] propose combining human, organizational and technical measures. The first includes awareness and training, the second policies and procedures and the last one includes automated measures to detect phish.

Such a multi-pronged approach is clearly superior to any approach that relies solely on either shoring up technical measures or human training. The proposal we presented in this paper still has a role to play in reducing the cyber-defense deficit, but we do not claim this to be sufficient in reducing the deficit. The one thing we cannot do is to rely solely on security awareness training, even if we make it as effective as it can be.

Kok *et al.* [65] explain that the intervention mapping methodology guarantees that: (1) interventions are grounded on empirical evidence and theory; (2) the intervention is linked to both the theory and the identified issues; (3) the stakeholders identify the issues to be addressed; (4) the intervention is properly targeted; and (5) the methodology ensures that intervention implementation issues are contemplated and accommodated throughout the design of the intervention.

VII. Conclusion

In this paper we have explained why security awareness training is required. We reviewed the research literature on training, in terms of design, formulation and delivery of the training. We highlighted the fact that the training might fail because it is not formulated to address behavioral aspects. We proposed a different approach, designed to target specific behaviors, and to exploit known behavioral change mechanisms. We illustrated the application thereof with an example. We present this proposal to open a discourse in the community so that we can move towards more effective awareness training.

Acknowledgement

This research was carried out while the first author was a Fulbright Scholar at Mississippi State University.

References

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] D. Aitel. Why you shouldn't train employees for security awareness. Immunity Inc. http://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html, 2012.

[3] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Usenix Security*, pages 257–272, 2013.

[4] E. Albrechtsen and J. Hovden. The information security digital divide between information security managers and users. *Computers & Security*, 28(6):476–490, 2009.

[5] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, 29(4):432–445, 2010.

[6] S. Allam, S. V. Flowerday, and E. Flowerday. Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42:56–65, 2014.

[7] C. Ammendolia, D. Cassidy, I. Steenstra, S. Soklaridis, E. Boyle, S. Eng, H. Howard, B. Bhupinder, and P. Côté. Designing a workplace return-to-work program for occupational low back pain: an intervention mapping approach. *BMC Musculoskeletal Disorders*, 10(1):1, 2009.

[8] E. B. Kim. Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 22(1):115–126, 2014.

[9] P. Balozian, D. Leidner, and M. Warkentin. Compliance-inducing techniques: Differentiating managers and employees. *Journal of Computer Information Systems*. forthcoming.

[10] A. Bandura. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, 84(2):191, 1977.

[11] L. K. Bartholomew and P. D. Mullen. Five roles for using theory and evidence in the design and testing of behavior change interventions. *Journal of Public Health Dentistry*, 71(s1):S20–S33, 2011.

[12] M. Bateson, L. Callow, J. R. Holmes, M. L. R. Roche, and D. Nettle. Do images of 'watching eyes' induce behaviour that is more pro-social or more normative? a field experiment on littering. *PloS one*, 8(12):e82055, 2013.

[13] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. Passwords and the evolution of imperfect authentication. *Commun. ACM*, 58(7):78–87, June 2015.

[14] J. C. Brancheau, B. D. Janz, and J. C. Wetherbe. Key issues in information systems management: 1994-95 SIM Delphi results. *MIS quarterly*, pages 225–242, 1996.

[15] B. Brown. FTC flouts conventional wisdom, says changing passwords often can do harm. http://www.digitaltrends.com/computing/federal-trade-commission-ftc-computer-password-changing-bad-idea/, 2016.

[16] T. C. Brown. Loss aversion without the endowment effect, and other explanations for the wta–wtp disparity. *Journal of Economic Behavior & Organization*, 57(3):367–379, 2005.

[17] J. Brug, A. Oenema, and I. Ferreira. Theory, evidence and intervention mapping to improve behavior nutrition and physical activity interventions. *International Journal of Behavioral Nutrition and Physical Activity*, 2(1):2, 2005.

[18] H. Cavusoglu, B. Mishra, and S. Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1):70–104, 2004.

[19] Y. Chen, K. Ramamurthy, and K.-W. Wen. Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, 29(3):157–188, 2012.

[20] M. Ciampa. A comparison of password feedback mechanisms and their impact on password entropy. *Information Management & Computer Security*, 21(5):344–359, 2013.

[21] N. Clarke, S. Furnell, G. Stewart, and D. Lacey. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1):29–38, 2012.

[22] M. Costanzo, D. Archer, E. Aronson, and T. Pettigrew. Energy conservation behavior: The difficult path from information to action. *American psychologist*, 41(5):521, 1986.

[23] J. D'Arcy and A. Hovav. Deterring internal information systems misuse. *Communications of the ACM*, 50(10):113–117, 2007.

[24] J. D'Arcy, A. Hovav, and D. Galletta. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1):79–98, 2009.

[25] M. B. Desman. The ten commandments of information security awareness training. *Information Systems Security*, 11(6):39–44, 2003.

[26] S. I. Detaille, J. W. van der Gulden, J. A. Engels, Y. F. Heerkens, and F. J. van Dijk. Using intervention mapping (IM) to develop a self-management programme for employees with a chronic disease in the Netherlands. *BMC Public Health*, 10(1):1, 2010.

[27] R. DeVries. Vygotsky, Piaget, and education: A reciprocal assimilation of theories and educational practices. *New ideas in Psychology*, 18(2):187–213, 2000.

[28] A. Dijksterhuis, J. A. Bargh, and J. Miedema. Of men and mackerels: Attention, subjective experience, and automatic social behavior. In H. Bless and J. Forgas, editors, *The message within: The role of subjective experience in social cognition and behavior*, chapter 3, pages 37–51. Psychology Press, New York, 2000.

[29] R. C. Dodge, C. Carver, and A. J. Ferguson. Phishing for user security awareness. *Computers & Security*, 26(1):73–80, Elsevier, 2007.

[30] A. Edland and O. Svenson. Judgment and decision making under time pressure. In *Time pressure and stress in human judgment and decision making*, pages 27–40. Springer, 1993.

[31] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2379–2388, Paris, 2013. ACM.

[32] M. Elder. Russian guard service reverts to typewriters after NSA leaks. https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks, 2013.

[33] A. Elise. Another ransomware attack shuts down an entire county's government. http://www.wtae.com/article/another-ransomware-attack-shuts-down-an-entire-countys-government/8678812, 2017.

[34] M. M. Eloff and S. H. von Solms. Information security management: a hierarchical framework for various approaches. *Computers & Security*, 19(3):243–256, 2000.

[35] M. Eminağaoğlu, E. Uçar, and Ş. Eren. The positive outcomes of information security awareness training in companies–a case study. *information security technical report*, 14(4):223–229, 2009.

[36] Ernst and Young. Global information security survey 2016-17. http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016, 2017.

[37] J. S. B. Evans. *Bias in human reasoning: Causes and consequences.* Lawrence Erlbaum Associates, Inc, 1989.

[38] J. Eyers. Banks test staff with cyber security 'fire drills'. 14 Sept http://www.afr.com/technology/banks-test-staff-with-cyber-security-fire-drills-20160914-grg2e8, 2016.

[39] J. Ferrara. Ten commandments for effective security training. http://www.csoonline.com/article/2131688/security-awareness/ten-commandments-for-effective-security-training.htmlTencommandmentsforeffectivesecuritytraining, 2012.

[40] M. Finger. From knowledge to action? Exploring the relationships between environmental experiences, learning, and behavior. *Journal of social issues*, 50(3):141–160, 1994.

[41] W. R. Flores, E. Antonsen, and M. Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43:90–110, 2014.

[42] E. D. Frauenstein and R. von Solms. Phishing: How an Organization can Protect Itself. In *Information Security South Africa Conference*, pages 253–268. Information Security South Africa, 2009.

[43] S. Furnell and N. Clarke. Organizational security culture: Embedding security awareness, education, and training. *Proceedings of the IFIP TC11 WG*, 11:67–74, 2005.

[44] S. Furnell, M. Gennatou, and P. Dowland. A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6):352–357, 2002.

[45] A. Ghoshal. Hackers use ransomware to target hotel guests' door locks. https://thenextweb.com/security/2017/01/30/hackers-use-ransomware-to-lock-hotel-guests-in-their-rooms/, 2017.

[46] S. Goel, M. Warkentin, K. Williams, and K. Renaud. Does Risk Disposition Play a Role in Influencing Decisions to Behave SECUREly? In *IFIP Dewald Roode Workshop. University of New Mexico, Albuquerque.*, 2016. October 7-8. http://ifip.byu.edu/ifip2016.html.

[47] G. A. Guagnano, P. C. Stern, and T. Dietz. Influences on attitude-behavior relationships a natural experiment with curbside recycling. *Environment and behavior*, 27(5):699–718, 1995.

[48] D. Halpern. *Inside the Nudge Unit: How small changes can make a big difference*. WH Allen, London, 2015.

[49] C. Horne. Lack of cyber security knowledge leads to lazy decisions from executives. https://theconversation.com/lack-of-cyber-security-knowledge-leads-to-lazy-decisions-\\from-executives-68065, 2016.

[50] A. Hovav and P. Gray. The ripple effect of an information security breach event: a stakeholder analysis. *Communications of the Association for Information Systems*, 34(50):893–912, 2014.

[51] P. Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95, 2012.

[52] ISO. Iso/iec 17799:2005 information technology – security techniques – code of practice for information security management. http://www.iso.org/iso/catalogue_detail?csnumber=39612.

[53] K. Jansson and R. von Solms. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584–593, 2013.

[54] E. C. Johnson. Security awareness: switch to a better programme. *Network Security*, 2006(2):15–18, 2006.

[55] A. C. Johnston, M. Warkentin, and M. T. Siponen. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1):113–134, 2015.

[56] D. Kahneman, J. L. Knetsch, and R. H. Thaler. Anomalies: The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives*, 5(1):193–206, 1991.

[57] K. Kannan, J. Rees, and S. Sridhar. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, 12(1):69–91, 2007.

[58] D. E. Kanouse and I. Jacoby. When does information change practitioners' behavior? *International journal of technology assessment in health care*, 4(01):27–33, 1988.

[59] C. Kern. Ransomware attack results in loss of 8 years' worth of evidence for police department. http://www.zdnet.com/article/ransomware-is-about-to-get-a-lot-worse-by-holding-your-operating-\\system-hostage/, 2017.

[60] M. Khonji, Y. Iraqi, and A. Jones. Phishing detection: a literature survey. *Communications Surveys & Tutorials, IEEE*, 15(4):2091–2121, IEEE, 2013.

[61] T. Klaus and J. E. Blanton. User resistance determinants and the psychological contract in enterprise system implementations. *European Journal of Information Systems*, 19(6):625–636, 2010.

[62] G. Kok, L. K. Bartholomew, G. S. Parcel, N. H. Gottlieb, and M. E. Fernández. Finding theory-and evidence-based alternatives to fear appeals: Intervention mapping. *International Journal of Psychology*, 49(2):98–107, 2014.

[63] G. Kok, N. H. Gottlieb, G.-J. Y. Peters, P. D. Mullen, G. S. Parcel, R. A. Ruiter, M. E. Fernández, C. Markham, and L. K. Bartholomew. A taxonomy of behaviour change methods: an intervention mapping approach. *Health Psychology Review*, pages 1–16, 2015.

[64] G. Kok, S. H. Lo, G.-J. Y. Peters, and R. A. Ruiter. Changing energy-related behavior: An intervention mapping approach. *Energy Policy*, 39(9):5280–5286, 2011.

[65] G. Kok, H. Schaalma, R. A. Ruiter, P. Van Empelen, and J. Brug. Intervention mapping: protocol for applying health psychology theory

to prevention programmes. *Journal of health psychology*, 9(1):85–98, 2004.

[66] H. Kruger, L. Drevin, and T. Steyn. A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5):316–327, 2010.

[67] H. A. Kruger and W. D. Kearney. A prototype for assessing information security awareness. *computers & security*, 25(4):289–296, 2006.

[68] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of Phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[69] K. Lewin et al. Field theory in social science. 1951.

[70] H. Liang, Y. Xue, and L. Wu. Ensuring employees' it compliance: Carrot or stick? *Information Systems Research*, 24(2):279–294, 2013.

[71] D. MacGregor. *The human side of enterprise*, volume 21. New York, 1960.

[72] R. R. McEachan, R. J. Lawton, C. Jackson, M. Conner, and J. Lunt. Evidence, theory and context: using intervention mapping to develop a worksite physical activity intervention. *BMC public Health*, 8(1):326, 2008.

[73] R. R. McEachan, R. J. Lawton, C. Jackson, M. Conner, D. M. Meads, and R. M. West. Testing a workplace physical activity intervention: a cluster randomized controlled trial. *International Journal of Behavioral Nutrition and Physical Activity*, 8(1):29, 2011.

[74] D. McKenzie-Mohr. Promoting sustainable behavior: An introduction to community-based social marketing. *Journal of Social Issues*, 56(3):543–554, 2000.

[75] D. McKenzie-Mohr. *Fostering sustainable behavior: An introduction to community-based social marketing*. New society publishers, 2013.

[76] S. Michie, M. Johnston, J. Francis, W. Hardeman, and M. Eccles. From theory to intervention: mapping theoretically derived behavioural determinants to behaviour change techniques. *Applied Psychology*, 57(4):660–680, 2008.

[77] NCSC. The problems with forcing regular password expiry. https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry, 2015.

[78] L. H. Newman. Ransomware turns to big targets—with even bigger fallout. https://www.wired.com/2017/02/ransomware-turns-big-targets-even-bigger-fallout/, 2017.

[79] D. Pauli. Go phish your own staff: Dev builds open-source fool-testing tool. http://www.theregister.co.uk/2016/02/04/no_more_excuses_dev_builds_dead_easy_open_source_antiphishing_app/, 2016. Accessed 15 Sept 2016.

[80] T. R. Peltier. Implementing an information security awareness program. *Information Systems Security*, 14(2):37–49, 2005.

[81] J. A. Pooley and M. O'Connor. Environmental education and attitudes emotions and beliefs are what is needed. *Environment and behavior*, 32(5):711–723, 2000.

[82] B. Reinheimer, M. Volkamer, and K. Renaud. User Experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & Security*, 2017. To Appear.

[83] Y. Rezgui and A. Marks. Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7):241–253, 2008.

[84] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65–78, 2015.

[85] R. Samani. 34% NHS Trusts Have Been Hit By Ransomware Over Past 18 Months. http://www.informationsecuritybuzz.com/expert-comments/34-nhs-trusts-hit-ransomware-past-18-months/, 2017.

[86] E. H. Schein. *Organizational culture and leadership*, volume 2. John Wiley & Sons, 2010.

[87] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1):92–100, 2009.

[88] A. Sotirakopoulos. *Influencing user password choice through peer pressure*. PhD thesis, The University Of British Columbia (Vancouver), 2011.

[89] A. Stephanou. *The impact of information security awareness training on information security behaviour*. PhD thesis, University of the Witwatersrand, 2009.

[90] P. C. Stern and E. Aronson. *Energy use: The human dimension*. WH Freeman and Company, New York, NY, 1984.

[91] T. Steyn, H. A. Kruger, and L. Drevin. Identity theft. Empirical evidence from a Phishing exercise. In *IFIP International Information Security Conference*, pages 193–203. Springer, 2007.

[92] D. W. Straub and R. J. Welke. Coping with systems risk: security planning models for management decision making. *MIS quarterly*, pages 441–469, 1998.

[93] R. H. Thaler and C. R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press, 2008.

[94] M. E. Thomson and R. von Solms. Information security awareness: educating your users effectively. *Information management & computer security*, 6(4):167–173, 1998.

[95] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, and N. Christin. How does your password measure up? the effect of strength meters on password creation. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*, pages 65–80, Bellevue, 2012. USENIX.

[96] J. A. Valentine. Enhancing the employee security awareness model. *Computer Fraud & Security*, 2006(6):17–19, 2006.

[97] S. H. van Oostrom, J. R. Anema, B. Terluin, A. Venema, H. C. de Vet, and W. van Mechelen. Development of a workplace intervention for sick-listed employees with stress-related mental disorders: Intervention mapping as a useful tool. *BMC health services research*, 7(1):127, 2007.

[98] A. Vance, D. Eargle, K. Ouimet, and D. Straub. Enhancing password security through interactive fear appeals: A web-based field experiment. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pages 2988–2997, Hawai'i, 2013. IEEE.

[99] B. Von Solms and R. Von Solms. The 10 deadly sins of information security management. *Computers & Security*, 23(5):371–376, 2004.

[100] C. Vroom and R. von Solms. A practical approach to information security awareness in the organization. In *Security in the Information Society*, pages 19–37. Springer, 2002.

[101] M. Wilson and J. Hash. Building an information technology security awareness and training program. *NIST Special publication*, 800:50, 2003.