HORNETSECURITY

EMPLOYEE SECURITY INDEX

WHITEPAPER

Social engineering - users as the way in

As companies and institutions continue to improve their IT defenses using technology, the number of social engineering attacks has exploded around the world. Back in 2013, just 17% of all cyber attacks had a social engineering component, while today, social engineering paves the way for the vast majority of attacks. The extent and sophistication of some of these attacks is clear to see—take the huge spread of the malware Emotet and its successors, for example. Emotet specifically infiltrates contact details and e-mail content in infected mailboxes, and uses this information to spread further. These kinds of spear phishing e-mails can be almost impossible for non-experts to identify.

Security awareness strengthens the "human firewall"

The human factor is crucial in any approach to information security - the key concept here being "security awareness". Security awareness describes the extent to which employees are aware of the importance of information security at their company and the essential role they play in this respect, particularly through their conduct.

There are a whole host of measures that can be used to boost security awareness. What's important here is to see users not as a risk, but rather as a fundamental part of the IT security solution - "You are your company's firewall". This means engaging employees in the process, not overburdening them and, in particular, not scaring them.

Planning measures to raise security awareness, however, can involve a number of challenges.

- How do you make sure that security awareness measures are effective in the long term?
- Is there any return on investment? In other words, is the investment worthwhile?
- Is there a benchmark or comparison with other organizations in similar sectors?
- Can training be customized to employees in a particular organization, rather than a one-size-fits-all approach?

The Employee Security Index - ESI® for short - makes the security behavior of employees reproducibly measurable using realistic scenarios and standardized methodology. This White Paper details the patented procedure for determining the ESI® and presents a benchmark from over 60 European companies.

Categorization of attacks provides the basis for a standardized measuring method

To make security awareness measurable, realistic simulation of spear phishing attacks is absolutely essential. Individual attacks should also be comparable with one another—only then can measurement over the long term yield conclusive results about the development of security awareness.

This is why the underlying phishing scenarios are graded into different categories. The key factor in such categorization is the time an attacker needs to invest in preparing and executing an attack scenario, for example, in the procurement of information (OSINT), technical preparation, copying of website designs, and keeping the infrastructure ready. On this basis, phishing scenarios can be divided into seven categories (known as levels) requiring different amounts of preparation.

Level	Example	Preparation time
1	Typical mass phishing e-mail such as order confirmation from a well-known shopping portal	approx. 15 minutes
2	E-mail purporting to be from senior manager (CEO fraud)	approx. 1 hour
3	Spear phishing e-mail incorporating public information about the company, e.g. from employer review sites	approx. 2 hours
4	Spear phishing e-mail referencing the recipient's department or role, e-mail from direct colleagues or managers.	approx. 4 hours
5	Spoofed e-mail from a business partner, who has not activated e-mail spoofing protection or whose account has been hacked.	approx. 6 hours
6	A business partner or colleague has been hacked. E-mail from a personal contact replying to a previous e-mail conversation.	approx. 12 hours
7	Spear phishing e-mail referencing things the recipient is currently working on, e.g. a status update on an ongoing project in which the recipient is involved.	More than 20 hours

Table: Overview of preparation time

Security awareness indicator: ESI®—the Employee Security Index

In order to measure the awareness of a test group, each participating employee becomes the target of randomly selected attack scenarios from different categories. The "success rate" (from the point of view of the attacker) is then measured across the test group.

Expecting a "success rate" of 0 to be achieved is unrealistic - people make mistakes. That's why we define an "exemplary" test group, which lies on the boundary between security and feasibility. Based on the time an attacker needs to invest in preparation, we define tolerance values, within which the security behavior of employees can still be regarded as "exemplary". For categories 1 through 7, these tolerance values are between 1.1 and 6.2%.

An exemplary test group with these exact success rates achieves an ESI® of 90. If critical behavior is exhibited twice as often as in the exemplary group, e.g. by clicking a harmful link in a phishing e-mail, the group achieves an ESI® of 80; if critical behavior is exhibited three times as often, the group only achieves an ESI® of 70. Values below 70 are regarded as critical (see Figure 1).

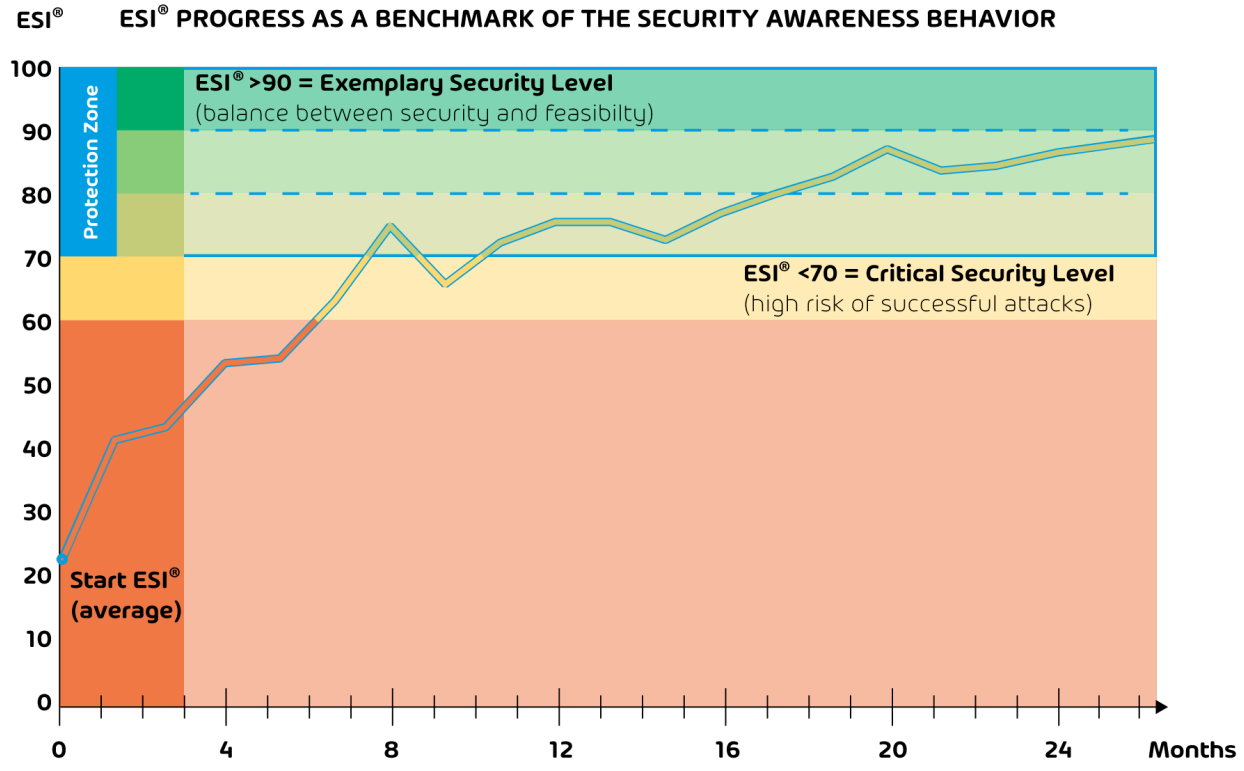

Figure 1: A sample progression of ESI® over time as a benchmark for security culture

Determination of ESI® in European companies indicates a lack of security awareness—but significant improvements through training are measurable.

Using phishing simulations, the Employee Security Index has been determined in internationally operating companies and authorities since the middle of 2018— specifically by measuring the click rate on links and file attachments in this respect. Examples of simulated attacks include a message that pretends to be from the user's mailbox saying that their storage is full (Category 1), an e-mail from a random colleague containing a link to a funny GIF (Category 2), or an inquiry from the department manager about an invoice included as an attachment (Category 4). In these cases, the phishing simulation was made to be as realistic as possible, with all participants receiving individual spear phishing attacks at random times.

Analysis of over 1.7 million simulated phishing attacks provides a revealing insight into the security behavior of employees from companies of all sectors and sizes, as illustrated in Figure 2 for a period of 12 months.

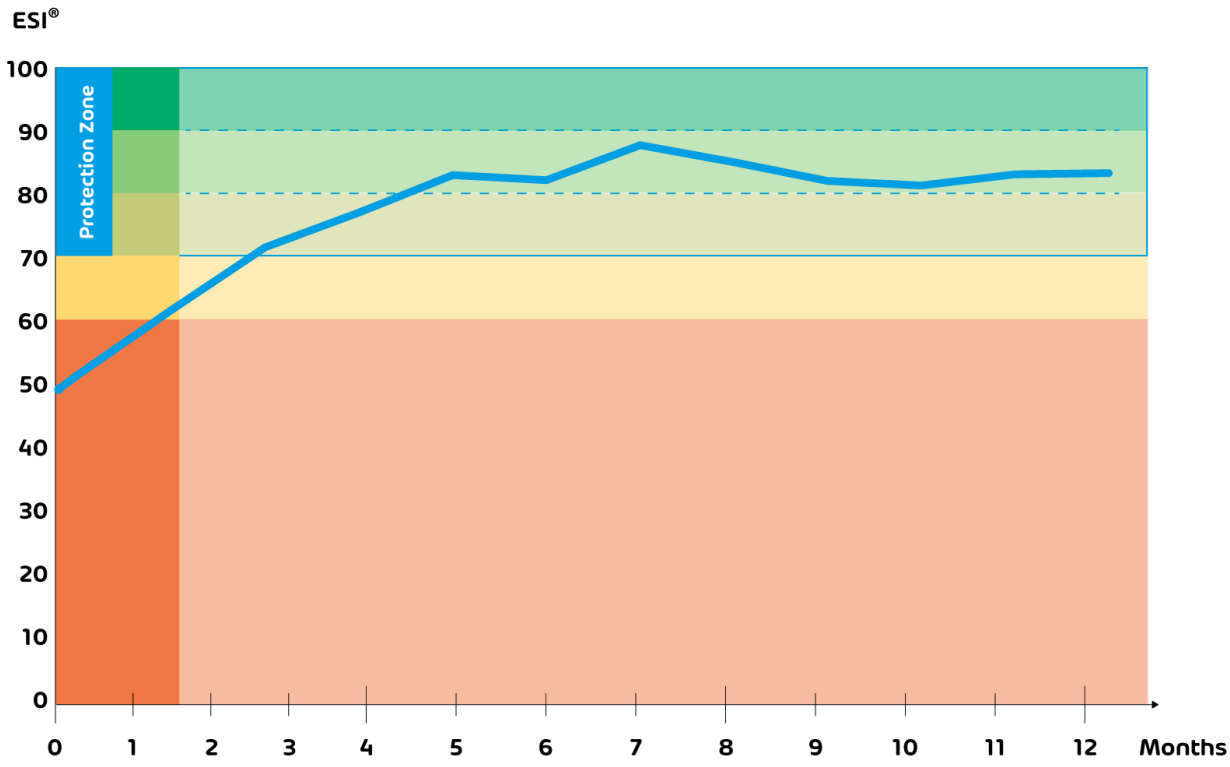

Figure 2: Determination of average ESI® from the phishing simulation

Continuous awareness training required

The average ESI curve over just the first 12 months highlights why continuous training is required to maintain a good level of security, including in the longer term. While the ESI curve rises sharply to start with and soon reaches an acceptable level of security, it becomes considerably more difficult to maintain this level as spear phishing scenarios become more sophisticated—particularly as new employees join the company or individual groups and employees pause their training, which can be seen in Figure 3.

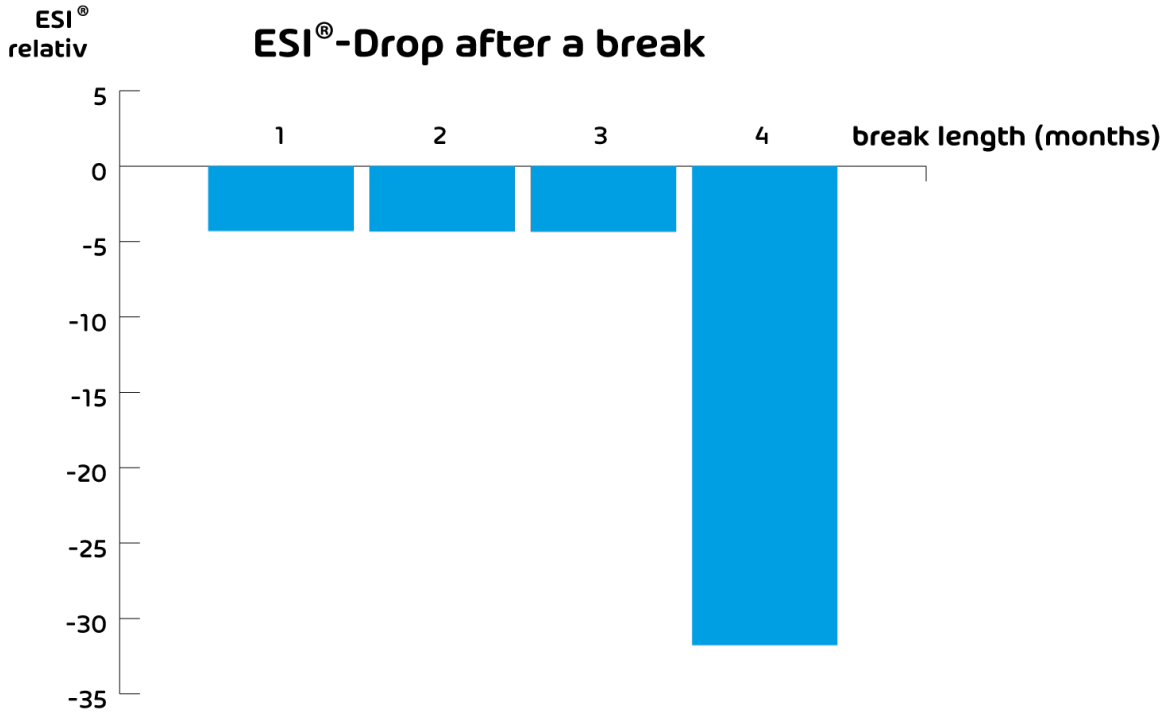

Figure 3: ESI® drop after a pause in training

Training to keep awareness high

Awareness is like a muscle that has to be trained regularly to prevent fatigue. With individual groups or employees who pause awareness training and resume it at a later time, there is a clear deterioration in security behavior. Without training, they become more negligent during the pauses and key training content is quickly forgotten. The alarming extent of this effect is clear from the ESI drop in the graphic. Even after a pause of just one month, ESI drops by 5 points, often falling below the target security level. After 4 months, ESI drops by over 30 points—and it's almost as if no awareness training had been undertaken at all.

Monitoring instrument as a basis for determining further security awareness measures

The ESI® is a monitoring instrument that can be used to continuously monitor security awareness in companies. The effectiveness of individual training measures can be reviewed and specific needs can be identified. Communication with both management and staff is facilitated by a tangible indicator. Quantitative analysis of security awareness provides a direct comparison with other companies in similar industries and can thus be used as a basis for decisions on further investments.

Employee training—fully automatic with the Security Awareness Suite

Raising employees' security awareness is essential for effective protection from cyber attacks. This is because technical security measures alone are insufficient when hackers know how to specifically exploit human vulnerabilities.

The job of many IT security managers nevertheless faces the challenge that long-term employee training can be time-consuming and use up a lot of resources. Our Security Awareness Suite relieves you from most of this burden.

Using the ESI® indicator for measurability, our Security Awareness Suite trains your employees in a needs-based, fully automatic manner for effective awareness raising in the long term. The continuous training program includes various methods for reaching employees effectively — from phishing simulations, e-tutorials and video clips to awareness materials. The result is a proactive security culture with informed employees, who are aware of their important role for the company and act accordingly. The Awareness Engine is the technological heart of our Security Awareness Suite and offers the right amount of training for every individual. Every participant receives as much training as is necessary and no more than is required.