CLTRe
a KnowBe4 company

KnowBe4 Research

Security Culture and Credential Sharing

How Improved Security Culture Reduces Credential Sharing in Cybersecurity

Anita-Catrin Eriksen
Gregor Petrič, PhD
Kai Roer

Table of Contents

Executive Summary

In 2020, most hacker attacks are successful because they apply social engineering: they make employees give away information that in turn give the hacker access to the computer systems of the employer. These attacks cost organizations millions of dollars every year, and may even cause them to go bankrupt.

Our groundbreaking research shows that security culture and security behaviors are closely linked. For the first time, this link has been demonstrated empirically, using large data sets on real people from around the world. Using evidence to prove that security culture and behavior are linked, is an important finding by itself.

Our research studies the impact that security culture has on secure behavior. The findings demonstrate that there are very important reasons to focus on improving security culture in organizations. There is 52 times the difference between the behaviors taken in the worst class (Poor) and the best class (Good). This difference is demonstrated by the number of employees entering their sensitive data during a simulated phishing attack. In the class Poor, employees on average enter data in 5.2% of the simulated phishing emails. In the class Good, this number is 0.1%. As organizations improve their security culture, the risky behaviors of their employees are reduced.

Conversely, if an organization sees a negative change in security culture by just one level (moving from *Good* to *Moderate*), the organization now sees an increase in risk by eight times.

Table: Change in Risky Behavior (Data Entry) by Improved Security Culture Score

	Mediocre	Moderate	Good
Poor	2x	6x	52x
Mediocre	—	3x	24x
Moderate	—	—	8x

To identify these patterns, we have looked at the data collected from 97,661 employees across 1,115 organizations. The dataset combines the measured behaviors of employees as measured using the KnowBe4 Kevin Mitnick Security Awareness Training (KMSAT) phishing assessment platform, and the measured security culture of the organizations of the same employees, as collected by the Security Culture Survey.

Improving security culture should be the number one strategy for organizations to protect themselves. There are a number of strategies organizations can implement to improve security culture, for example by automating phishing assessments and training of employees. A structured approach to manage the security culture should be implemented, and that approach should involve timely measurements to be taken by all employees.

This paper goes into great detail to explain how we arrived at these results.

Introduction

Social engineering, where human nature is being exploited, is the major attack vector being used in the increased number of organizations worldwide being attacked by criminals in the cyber domain[1]. These attacks are causing organizations to lose revenue, reputation and data, and are fast becoming the new normal in a global game that knows no borders. There is a need to understand the underlying human nature, both as individual beings and when individuals take part in groups, in order to build better protective measures for the industry.

In this paper, we examine the relationship between security culture and the different phishing activities as undertaken by employees of an organization. We examine the behavior and the reported security culture of 97,661 employees across 1,115 organizations, making this the largest and most complex study of the human factors relating to security to date.

Most of the previous work in this area focused on single subjects, like the effectiveness of phishing[2], the importance of culture to drive security[3], or were limited to survey-only data. Due to the nature of how most previous research, including our own, has been designed, no conclusive evidence has been provided that security culture has a (positive or negative) impact on employees' behavior.

In this study, we combine two different datasets. Both datasets include the same employees and organizations, which allows us to merge the datasets and provide simultaneous analysis of actual behaviors and security culture. We first examine the susceptibility to phishing attacks on individual employees across a large number of organizations. Next, we compare these findings with the security culture score of the organization the employees belong to. This novel approach allows us to provide empirical evidence that risky behavior (opening, clicking or entering data in a phishing email) is significantly reduced with better security culture. We show that the more severe the phishing action taken by the employee, the less likely this action is to be made in organizations with a security culture rated at the highest level. Conversely, the worse the security culture rating is, the more likely the employees are to put the organization at risk. The findings are not surprising, but it is the first time this has been demonstrated empirically at scale, using real-world data.

Phishing

Susceptibility to phishing emails is one of the key issues in the human factor of cybersecurity, as it is in the end, always an employee's decision whether to open the email, click on a link and enter some sensitive data into a fraudulent website. Nevertheless, such risky behavior of employees is according to scientific literature caused by three different categories of factors:

a) The characteristics of a phishing email, such as credibility, urgency, richness, authority.

b) Employees' characteristics, such as his/her personality, knowledge, curiosity, naivety, propensity to trust, being trained, experience, etc.

c) Organizational factors, such as security policies, work situations, organizational culture and security culture.[4]

1 The rise of social engineering attacks and why you must be vigilant. Web, accessed December 8th, 2020. https://www.fifosys.com/blog/security/the-rise-of-social-engineering-attacks-and-why-you-must-be-vigilant

2 Using Phishing Experiments and Scenario-based Surveys to Understand Security Behaviours in Practice, Waldo & al, 2013

3 From culture to disobedience: Recognising the varying user acceptance of IT security, S. Furnell, 2009

4 Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security and Privacy (IJISP), 9(1), 26-46.

Security Culture

Security culture has received substantial attention during the last decade both in academia and industry.[5] For example, in a 2020 study, 94% of organizations agreed that security culture is important.[6] Most academic papers to date have focused on understanding what influences and how to measure security culture. For example, research has found that when employees read the security policy, it can positively influence the security culture in the organization.[7] Security culture is often considered as a long-term investment that requires constant effort to maintain and grow.[8]

Contribution and Uniqueness of This Study

In recent years, (mostly scientific) research of factors of susceptibility to phishing emails has emerged. The validity of many of these findings is limited due to small samples of employees; focus on single or few organizations and industries; and/or limited to survey-only or experiment-only data. Consequently, the research findings cannot be generalized, are limited to specific industries and do not provide satisfactory insight into factors of susceptibility.

This study presents important methodological, statistical and conceptual advances compared to previous studies. The advances are highlighted below.

a) Large sample of employees (n=97,661), embedded within a large sample of organizations (n=1,115): Even more important than having a large sample of employees is having a large sample of different organizations. This is probably the biggest hindrance of existing research, which usually focuses only on one or few organizations or even on student samples, which cannot be a valid population for extrapolation to organizational contexts.

b) Integration of survey-based data and field-experiment data on phishing simulations: This allows anonymous linkage of employees' answers on survey questions with their actions on simulated phishing emails.

c) Distinction of different risky behaviors: opening a phishing email, clicking a link in a phishing email, opening an attachment in a phishing email, entering data on fraudulent websites. Other research is often focused only on a limited set of actions connected to simulated phishing emails (usually clicks on links in phishing emails). Our research considers and separates analysis of different actions pertaining to phishing emails: opening an email, clicking on a link, entering data on a simulated fraudulent website.

To our knowledge, no other study exists in the time of producing this report that would include the above mentioned elements, alone or combined.

---

5 A systematic review of scales for measuring information security culture. Information and Computer Security.

6 The Security Culture Report 2020 by KnowBe4 Research and CLTRe, a KnowBe4 Company.

7 Adéle Da Veiga, (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. Information & Computer Security, 24(2), 139-151.

8 Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. Journal of Organizational Computing and Electronic Commerce, 29(1), 4-23.

Methodology

This research is an integration of survey-based data[9] and field-experiment data of phishing simulations. We anonymously linked the answers employees provided in survey questions to their actions on simulated phishing attacks. Data was collected using the Security Culture Survey (SCS) and simulated phishing attacks of employees who are part of KnowBe4 customer organizations. Both these metrics are available within the KnowBe4 security awareness management platform KMSAT.

KnowBe4 offers its customers a wide variety of choices when it comes to sending out simulated phishing emails. Customers can choose and customize more than 5,000 phishing templates. The phishing template specifies the design and content of the phishing email (e.g., subject line, sender, message, etc.). It is also possible to decide the level of difficulty you want a phishing email to have on a scale from one to five. For each sent simulated phishing email, detailed data on the activities of the user is collected. The data collected includes:

- When phishing email was sent
- When (if) it was opened
- When (if) a link in the email was activated
- When (if) an attachment in the email was opened
- When (if) data was entered on the simulated fraudulent website
- When (if) the email was reported

In this report, we focus on the activities of opening email, clicking on links and entering data. The information about these activities was aggregated on the level of employees.

The Security Culture Survey (SCS) is a scientific measurement instrument developed by CLTRe.[10] It consists of 28 items that measure seven core dimensions of security culture. Scores are aggregated on an organizational level and transformed into a single variable, the Security Culture Score. The Security Culture Score ranges from 0 to 100. In the analyzed sample, organizations had a security culture score ranging from 39 to 90. Organization were categorized into four classes based on their security culture score:[11]

90 up to 100	**Excellent**[12]
80 up to 90	**Good**
70 up to 80	**Moderate**
60 up to 70	**Mediocre**
0 up to 60	**Poor**

9 The survey data is collected using the Security Culture Survey, a methodology researched and developed by Dr. Gregor Petrič and Kai Roer.

10 To Measure Security Culture, CLTRe, 2017: https://get.clt.re/whitepaper-to-measure-security-culture-a-scientific-approach

11 This is the same categorization which is used in the Security Culture Report 2020, with the exception of Moderate which has been divided here into two categories: Mediocre, and Moderate.

12 No organizations had an Excellent Security Culture Score in this study.

Data

In total, 97,661 employees and 1,115 organizations were analyzed. Only employees who received their first simulated phishing email in 2019 or 2020 were included. Organizations with less than 10 employees were excluded. All the phishing emails these employees received in 2019 and 2020 were included in the analysis.

Results

We analyzed the impact of the organization's security culture on employees' results on simulated phishing attacks. For the analysis, we used the analysis of variance-approach, with post-hoc Bonferroni Pairwise tests. The results show that there is a strong association between security culture and risky behavior. In organizations with "Good" security culture, employees click on links and enter data on simulated fraudulent sites less often than those with a Moderate or Poor security culture. The strongest effect of security culture was observed for entering data. This provides empirical evidence that having a Good security culture is essential for managing the ongoing problem of social engineering.

In this section, the detailed results of the analysis are presented. The average percentage of phishing activities for all employees depends on the security culture score. The average percentage of phishing activity per employee is calculated according to the below formula:

$$\bar{\mu}_{\%} = \frac{\sum_1^n PH_i}{n}$$

% = Average percentage of phishing activities per employee

PHi = Phishing activity (open, click, enter data) realized (1) or not (0)

n = number of all received phishing emails per employee

Here's a simple explanation for those who do not like formulas: Imagine a situation where two employees in an organization both received 10 phishing emails. The first employee clicked on a link in five emails while the second one clicked on a link in 0 emails. The average percentage of risky behavior (clicking) for the first employee is 50%, while for the second employee it is 0%.

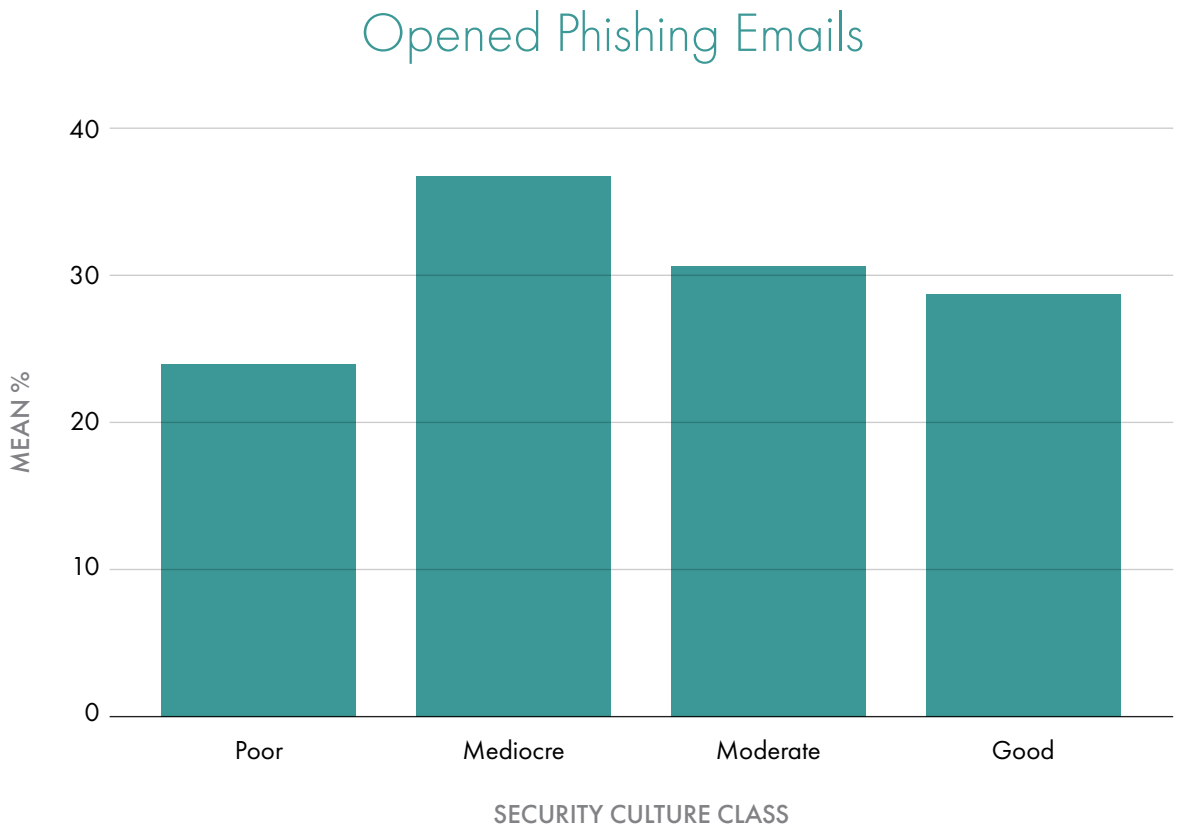
Opened Phishing Emails

When looking at the opening of emails, we note that there are few differences between the classes. Interestingly, the class that shows the least opening of emails is the class Poor security culture (24.1%). No other class shows that low open rate. However, when looking at the rate for clicking and for data entry, the same class demonstrates the worst behaviors of all classes. If we observe the differences in opening phishing emails across the other three classes, the data shows a pattern of reduction of openings as we move towards the class Good security culture.

Another observation to be made when considering the opening of phishing emails is the reasonable closeness in mean percentage of opened phishing emails across the classes, from 24.1% to 36%, with the total being 32.3%. We believe these numbers may be explained by the fact that most employees working with email are likely to open emails they receive in order to decide what action to take on that email. This area is, however, something that should be further researched.

Table: Security Culture Classes Showing the Opening of Phishing Emails in % [13]

SCS Class	Mean % of Opened
Poor	24.1%[a]
Mediocre	36.0%
Moderate	30.4%[b]
Good	28.5%[ab]
Total/Whole Sample	32.3%



13 Note: Differences between classes with the same superscript are not statistically significant. In all other cases the differences between classes are statistically significant.

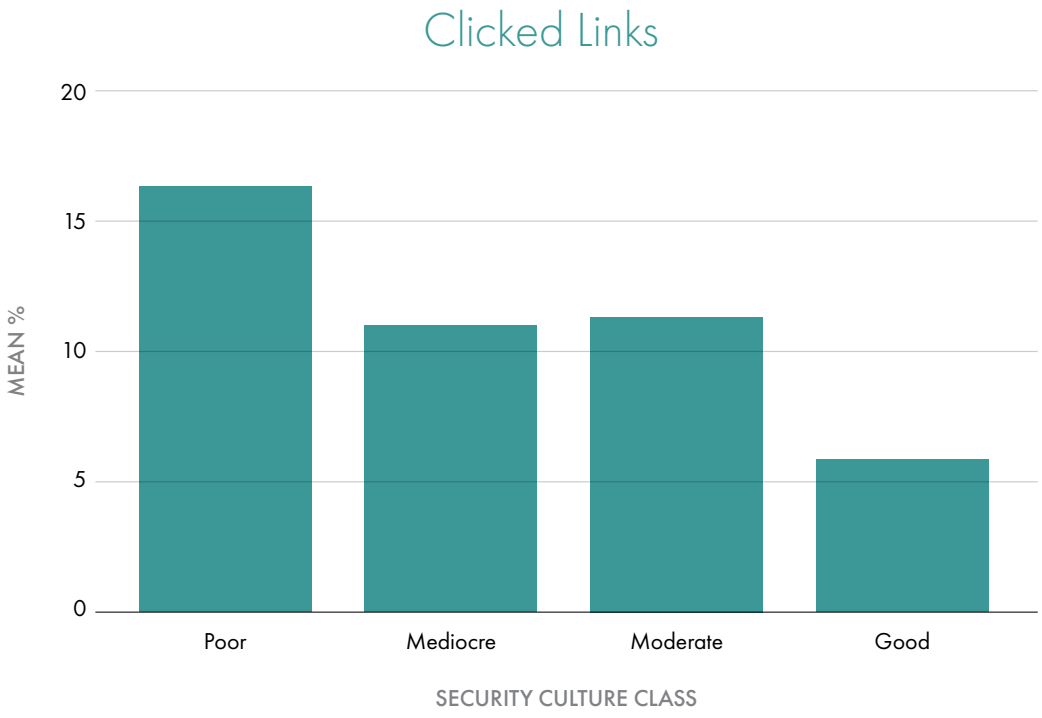
Clicked Links

Clicked links refer to employees who click on links in simulated phishing emails. When the data is examined, there is a clear pattern emerging: the worse the security culture, the higher the number of employees who will click on links in phishing emails. The good news is that the number of people clicking on links is significantly reduced by improving security culture. In organizations with Poor security culture, employees on average click on links in 16.4% of cases of simulated phishing emails which they receive. However, in the class Good security culture, employees on average click links in 6.1% of cases of phishing emails which they receive.

The percentage of clicked links generally decreases as security culture increases. The one exception in this trend is the class Mediocre and Moderate where the Bonferroni post-hoc test[14] shows that there was not a significant difference in the scores between these two classes (p = .932). This means that the observed difference between these means can be explained by chance.

Table: Security Culture Classes Showing the Clicked Links in %[15]

SCS	Mean % of Clicked Links
Poor	16.4%
Mediocre	11.2%[a]
Moderate	11.4%[a]
Good	6.1%
Total/Whole Sample	11.3%



14 The Bonferroni test is a statistical test used to reduce the instance of a false positive.

15 Note: Differences between classes with the same superscript are not statistically significant. In all other cases the differences between classes are statistically significant.

Data Entered

Data entered refers to employees who entered data on a simulated fraudulent website, which they were taken to by a simulated phishing email. The analysis shows that the strongest effect of security culture on phishing is in the case of entering data. In organizations with Poor security culture, employees on average enter data in 5.2% of cases of phishing emails which they receive. This percentage significantly declines with increasing security culture. In organizations with Good security culture, employees on average enter data in only 0.1% of cases of phishing emails which they receive.

Table: Security Culture Classes Showing the Data Entered in %

SCS	Mean % of Data Entered
Poor	5.2%
Mediocre	2.4%
Moderate	0.8%
Good	0.1%
Total/Whole sample	1.4%

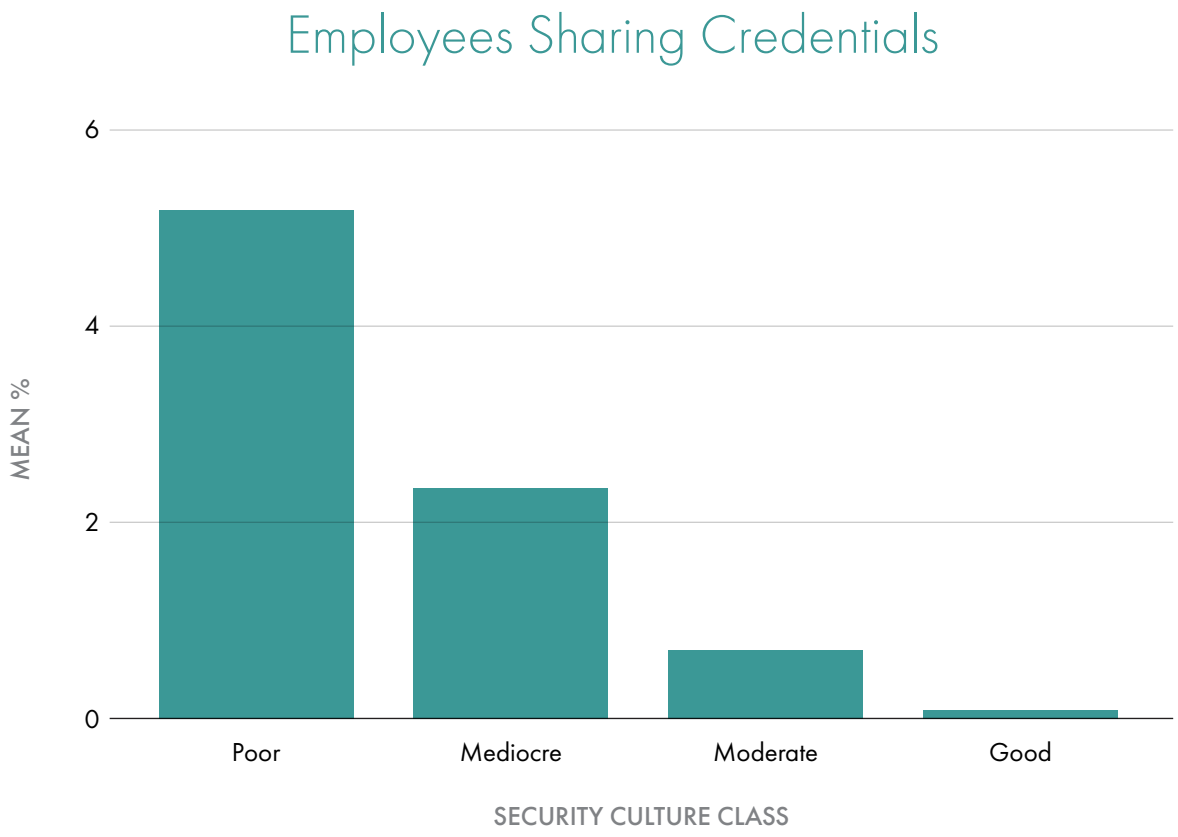
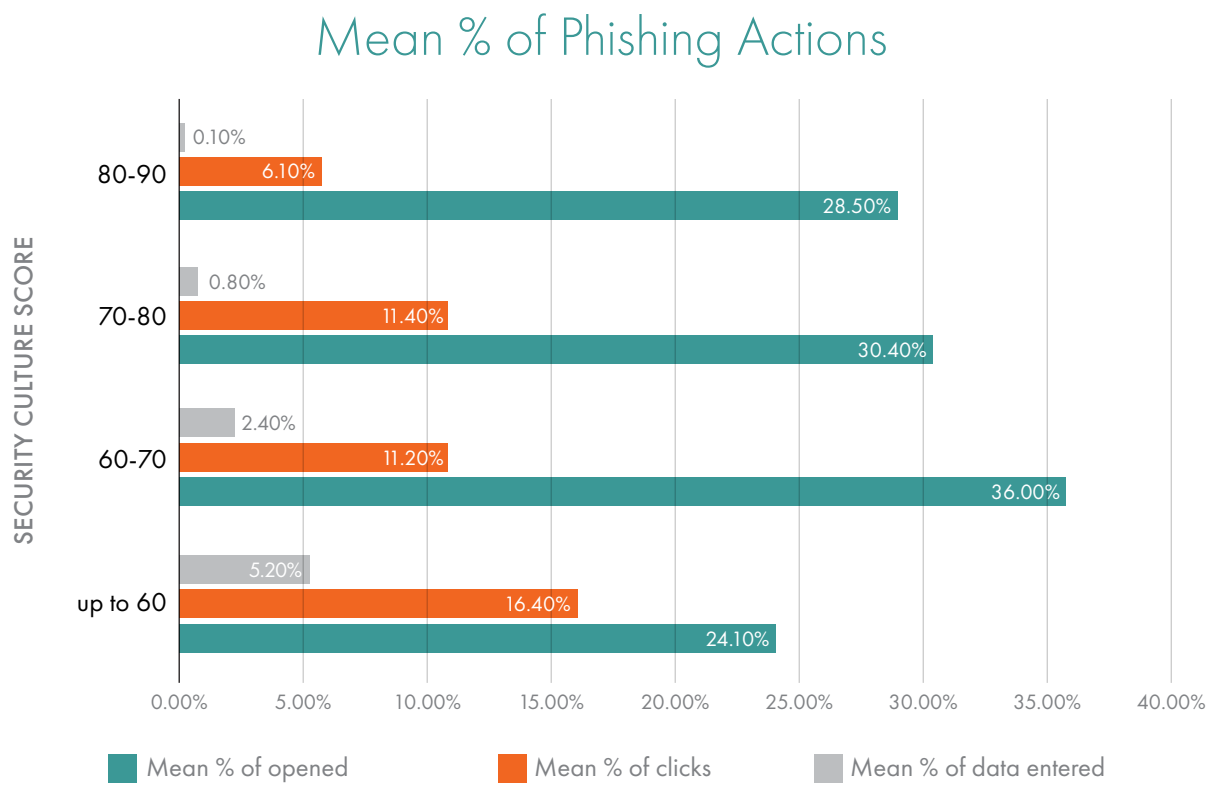


Table 1: Mean % by SCS Class

SCS	Mean % of Opened	Mean % of Clicks	Mean % of Data Entered
Poor	24.1%	16.4%	5.2%
Mediocre	36.0%	11.2%	2.4%
Moderate	30.4%	11.4%	0.8%
Good	28.5%	6.1%	0.1%
Total	32.3%	11.3%	1.4%



Risk Matrix

The implications of the findings in this document become even stronger when visualizing the change in risk associated with moving from one security culture class to another. The change in risk is evident through all the different actions taken, as explored in the previous chapter. In this section, focus is emphasized on the group of employees who enter data in a phishing scenario. This action is the most critical one from a security perspective, and also the one with the most dramatic improvement as the security culture improves.

Exploring the evidence, there are significant changes in activity when moving up through the security culture classes, regardless of which class that movement starts in. Organizations that are in the class Poor (5.2% of employees enter data) have 52 times as much risky behaviors as those organizations in the class Good (0.1% of employees enter data). This pattern is demonstrated across all the classes of security culture.

The differences in the risk of employees entering data have been calculated for all classes in the table below Change in Mean Risky Behavior (Data Entry) by Improved Security Culture Score.

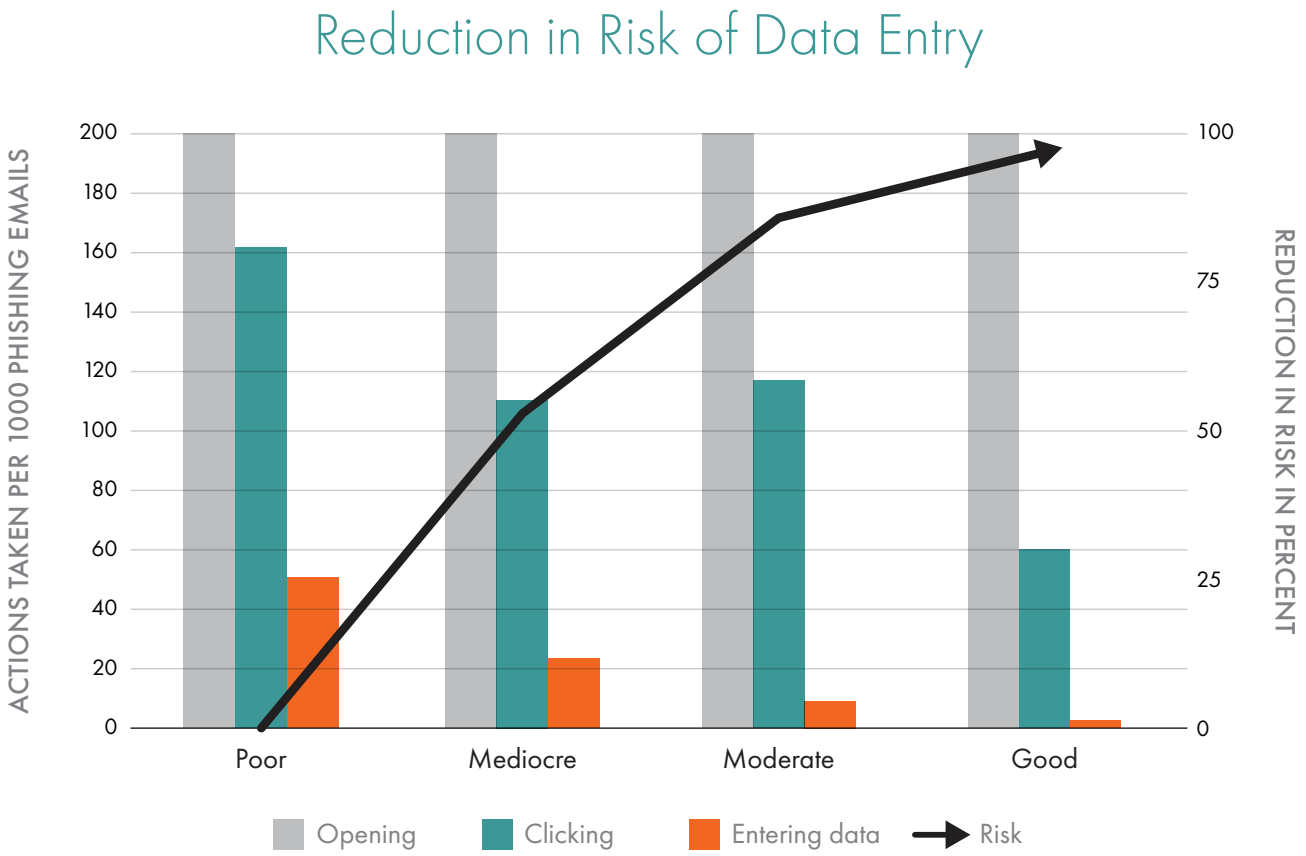
The table can be used to understand the extreme change in risky behavior that is seen when comparing organizations of different security culture classes. Even in the case of comparing the two classes that show the least differences (Mediocre to Poor), there is a difference of two times as much risky behavior from the class Mediocre to the class Poor. That is a doubling of risk. The class Moderate shows three times as much risky behavior as the class Mediocre, and six times as much as the class Poor. The most dramatic change is seen when comparing the class Good to the other classes. There is eight times as much data entry in the class Moderate, and 24 times as much data entry in the class Mediocre, and 52 times as much data entry in the class Poor, when compared to the best security culture class Good.

Table: Change in Mean Risky Behavior (Data Entry) by Improved Security Culture Score

	Mediocre	Moderate	Good
Poor	2x	6x	52x
Mediocre	--	3x	24x
Moderate	--	--	8x

The relative change in risk is illustrated in the graph below, where an upward shift in the security culture class (higher security culture score) results in reduced risk and a downward shift (lower security culture score) results in increased risk.

A significant reduction of risky behaviors is evinced by improving security culture. The differences are evident both in clicking and in entering data, as shown in the graph below.



This graph shows the number of actions (out of 1,000) taken by employees. The columns represent the different actions (Opening, Clicking, Entering Data), and the column groups represent the security culture class. The black line shows how the risk is reduced by moving from one class to another.

For readability, the graph has been transformed from percentages (per hundred) to promille (per thousand) due to the low number of data entered in the security culture class Good (Avg. 0.1% enter data). This means that employees on average enter data in one out of 1,000 phishing emails in the class Good. In the class Poor, employees will enter data in 52 out of 1,000 emails on average.

The graph has three columns in groups of four. Each light blue column represents the number of opening emails across the classes. Since the number of openings range from 241 of 1,000 phishing emails (24.1%) to 360 of 1,000 phishing emails (36%), the columns are all taller than the graph itself. The blue column represents the clicks with ranges from the class Good at 61 of 1,000 phishing emails (6.1%) to the class Poor at 164 of 1,000 phishing emails (16.4%). The orange column represents the data entry, with a range from the best class Good at 1 of 1,000 phishing emails (0.1%) to the worst class Poor at 52 of 1,000 phishing emails (5.2%).

The line that starts in the bottom-left corner (Poor) and points towards the upper right corner (Good), represents the change in risk for the organization. For the purpose of this study, risk is defined as the probability of a certain action (data entry) occurring in a security culture class during a given period. The risk is calculated by the relative difference between the percentages of actions taken (data entry). For the sake of simplicity, the class Poor was used as a benchmark, and all the numbers were compared to that class.

Suggestions for Actions Organizations Should Take

Based on the findings in this paper, the authors recommend that organizations work to improve their security culture, and that they measure the progress. There are a number of actions that can be taken to move to a better security culture class. These are some suggestions:

Risk Assessment

At regular intervals (annually or quarterly), complete, audit and update the organization's risk assessment plan. Use a combination of quantitative and qualitative methods to document the current situation, how it has changed from the previous situation and plan how to move forward. Make sure that your risk assessment includes the human factors as measured by security culture, knowledge and behavior of the organization and its employees.

Set up a Security Culture Program

Implement a security plan that includes a program designed to build and improve the seven dimensions of security culture.

Start With the Low Hanging Fruit

For many organizations, there are a number of opportunities to make fast progress and quick wins. One example is to implement a monthly phishing assessment program combined with targeted and relevant training content.

Automate the Mundane

As the threats evolve, it becomes increasingly difficult to track everything. Implementing automation for repetitive tasks is often possible. A monthly phishing assessment that automatically enrolls only the employees who need training, is often a good idea.

Engage With Your Peers

The security landscape is ever-changing and it is difficult to keep track of it all. Engage in the security community to learn from others, and to share your own knowledge and experience. Everyone wins!

Authors

Anita-Catrin Eriksen

Anita-Catrin Eriksen holds a Bachelor of Arts in Social Sciences and Humanities from University College Utrecht in the Netherlands. She also holds a Master of Science in Social Psychology from the University of Edinburgh in the UK. Her academic work mainly focused on attitudes, social identities, culture, statistics, and survey methodology. Eriksen is the research assistant at CLTRe, a KnowBe4 company. As the research assistant, she analyses data and conducts and advises on best practices for research. She works to ensure that insights into security culture and behavioral information security come from reliable and valid data.

Dr. Gregor Petrič

Dr. Gregor Petrič is an accomplished researcher and academic in the social scientific space, with a specialization in socio-informatics. He oversees that the research projects are of the required standard and quality. Petrič co-created the CLTRe security culture survey tool and analytics with Kai Roer. He is internationally well known for his advances in measurement of social science phenomena and applying structural models to explanation of internet-related social and cultural phenomena. He is also an expert in web survey methodology. He published numerous papers in top-end journals in the fields of information society, methodology of social science research and e-health. He serves as the head of the Centre for Methodology of Informatics (Faculty of Social Sciences, University of Ljubljana), where he was awarded full professor in 2019.

Kai Roer

Kai Roer (author of Build a Security Culture by publisher IT-Governance) has over 25 years of experience in cybersecurity, with much of his expertise centered around security culture. He is currently managing director of CLTRe, a KnowBe4 company, where he is responsible for security culture research. Prior to founding CLTRe, Roer created the global de facto standard Security Culture Framework. His groundbreaking research into security culture metrics provides organizations worldwide with deep insights into the human factors that influence risk and security. Roer is an award-winning specialist on security behaviors and security culture as well as a best-selling author. He is the host of the videocast "Security Culture TV" and an avid blogger. Roer keynotes at events around the world. He belongs to the Norway Chapter of the Cloud Security Alliance.

CLTRe, a Research Division of KnowBe4

CLTRe AS was established by Dr. Gregor Petrič and Kai Roer in 2015 in order to answer the information security industry´s need for a way to measure and understand the impact of security culture. The groundbreaking work is a prime example of applying science in the real world. In 2017, Aimee Laycock joined the team to help commercialize the platform. As a research-first company, CLTRe published the first Security Culture Report in 2017, measuring 11,212 employees in Northern Europe, at the time the largest global study into the human factors that influence security. Working with the EU, ENISA, SINTEF, and the Norwegian Research Council, CLTRe provided the industry with important facts and figures.

CLTRe AS was acquired by KnowBe4, Inc in 2019, and is committed to bringing our research to the world in order to help understand the human factors that influence security.

KnowBe4 Research

KnowBe4 Research is a special projects division of KnowBe4, Inc. Our mission is to provide IT and security leaders with high quality, vendor neutral data-driven insights related to cybersecurity and the human element.

KnowBe4, Inc.

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 34,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as the last line of defense.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

V011821