Whitepaper by CLTRe

To measure security culture

A scientific approach

Dr. Gregor Petrič and Kai Roer

Authors: Kai Roer, Dr. Gregor Petric
Layout and graphic design: CLTRe AS
Photos: Adobe Stock
Publisher: CLTRe North America, Inc.

Although the authors and publisher have made every effort to ensure that the information in this book was correct at press time, the authors and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Every effort has been made to contact copyright holders and to ensure that all information presented is correct. Some of the facts in this volume may be subject to debate or dispute. If proper copyright acknowledgment has not been made, or to communicate clarifications or corrections, please contact the publishers and we will correct the information in future re-printings, if any.

Whitepaper by CLTRe

Dr. Gregor Petric and Kai Roer

To measure security culture

A scientific approach

Contents

Introduction

Security incidents, and consequently security breaches and data loss, is on an old-time-high. With up to 95% of breaches being attributed to some human factor[1], it is clear that something must be done. Root cause analysis commonly trace breaches to weak culture that works against security.[2]

The Security Culture Framework defines security culture as the ideas, customs, and social behavior that "impact security in our organization, both in a positive and a negative way."[3] Organizations can leverage a strong security culture to help minimize security risk.

Given the ever-increasing digital threats they face, organizations have a strong reason to invest in their security culture. Many organizations find it difficult or are unaware of methods to measure their security culture, so they turn to measuring proxies, such as attendees and completion rates. These means of evaluation are not valid tools to assess

[1] Security Services 2014 Cyber Security Intelligence Index, IBM

[2] Kevin Beaver, "Make Security Culture Your Top Priority," Security Intelligence, IBM, last modified October 16, 2017, accessed October 18, 2017, https://securityintelligence.com/make-security-culture-your-top-priority/.

[3] "Definition of Security Culture," The Security Culture Framework, last modified September 4, 2014, accessed October 18, 2017, https://securitycultureframework.net/definition-of-security-culture/.

security culture and do not provide underlying information about how an organization's security culture has changed.

Changing and measuring security culture does not need to be difficult. Once a clear, scientifically backed method is developed, it can easily be deployed to assess security culture and act upon such assessment.

This whitepaper explains why security culture is an important concept by differentiating it from security awareness. Moreover, it sets forth why measuring the former matters to the business. It then discusses why measuring the human factor poses a problem to companies and argues that companies can adequately measure their security culture by relying on scientific methods. In support of that viewpoint, the whitepaper presents the scientific methodology of one approach in particular that is embedded in the CLTRe Toolkit.

Security Culture vs. Security Awareness

Many companies decide to invest in security awareness, or the process of educating employees about computer security.[4] By training and educating their employees about IT protection, organizations hope to leverage security awareness to help make each individual responsible for knowing the company's security policies.[5] Designated personnel responsible for upholding the security awareness program can then reinforce that message using a variety of media, audit the progress of the program, and make revisions as necessary.

The purpose of security awareness training is to train people with the hope they will change their security behavior. This hypothesis unfortunately doesn't have much empirical evidence. Changing security behaviors is difficult because organizations seek simple non-scientific answers to complex issues. Organizations habitually and consistently make many mistakes when setting about to change security related behaviors. Instead, organizations should draw upon social sciences, specifically psychological and social sciences. To be more successful with their initiatives, companies should build an organizational culture in which all employees engage one another as equal participants.

[4] Margaret Rouse, "security awareness training," TechTarget, last modified November 2011, accessed October 23, 2017, http://searchsecurity.techtarget.com/definition/security-awareness-training.

[5] Ryan Fahey, "Security Awareness -- Definition, History, And Types," Infosec Institute, accessed October 20, 2017, http://resources.infosecinstitute.com/category/enterprise/securityawareness/.

Why Measuring Security Culture Matters to the Business

Organizations can reap three main benefits from measuring their security culture on an ongoing basis.

Demonstrating effectiveness/value of investing in security culture

By evaluating their security culture, companies can track changes in their employees' behaviors and their underlaying factors. They can then use this progress to make additional decisions, such as identifying departments and teams for improvement or designating specific employees as potential insider threats. They can also leverage such change to justify additional security spending to executives and to achieve compliance with security regulations.

For example, Article 32 Section 1d of the General Data Protection Regulation (GDPR) mandates that organizations "ensure a level of security appropriate to the risk" by implementing "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."[6] Similarly, Article 47 Section 2n of the standard emphasizes the importance of "the appropriate data protection training to personnel having permanent or regular access to personal data."[7] These two provisions together mandate that all companies institute a security training program and evaluate the effectiveness of that framework. Measuring security culture and all efforts to strengthen it fulfill this requirement.

Reducing organizational risk

Organizations that measure security culture can expect to reduce their security risk. This outcome operates on two primary layers. First, regular evaluation of a company's security culture helps reinforce risk-averse behaviors and thereby improves overall security attitudes. Second, it advances the organization's security communication concerning digital threats both internally (among employees and contractors) and externally (to vendors, suppliers, and partners).

Gaining deep insights into the human factors

The *human factors* is a term used to describe different traits that individuals possess, and that in turn influences security and risk. It may pose a threat to organizations in that it can contribute to or cause security events, and it may pose an opportunity in that it can contribute to reduce risk and avoid security incidents. By measuring the human factors, organizations can monitor their changes over time and use the data to adapt different strategies and tactics on how to change the factors (i.e. improve them over time).

[6] "Article 32, EU GDPR, 'Security of processing,'" SecureDataService, accessed October 23, 2017, https://www.privacy-regulation.eu/en/32.htm.

[7] "Article 47, EU GDPR, Binding corporate rules,'" SecureDataService, accessed October 24, 2017, https://www.privacy-regulation.eu/en/47.htm.

Vanity Metrics and the MacNamara Fallacy

If organizations measure vanity metrics, they could ultimately fall into the McNamara Fallacy. This term refers to a situation where actors make decisions based solely on easily-obtainable quantitative data, such as employee attendance and completion rates, while ignoring other potentially more important aspects, such as qualitative features of a corporate security culture (which can also be quantified!). Pollster and thought leader Daniel vYankelovich framed his Fallacy in response to Robert MacNamara's belief that he could measure success in the Vietnam War based on body count:

> "The first step is to measure whatever can be easily measured. This is OK as far as it goes. The second step is to disregard that which can't be easily measured or to give it an arbitrary quantitative value. This is artificial and misleading. The third step is to presume that what can't be measured easily really isn't important. This is blindness. The fourth step is to say that what can't be easily measured really doesn't exist. This is suicide.[1]"

Just as body count does not necessarily signify success in war, how many employees attend or submit a completion form following security training does not help organizations measure the quality of or change in their security culture. Such vanity metrics do not, for example, evaluate employees' sense of responsibility to help defend the organization against digital threats. Neither do they account for operating norms that help bind employees together in their pro-security attitudes. These data points overall yield no information into how secure the culture of an organization is. Such metrics can be misleading and cause more harm when organization thinks it is secure, but in reality it is not.

[1] Will Friedman, "Dan Yankelovich Honored for Excellence in Public Opinion Research," Public Agenda, last modified November 19, 2015, accessed October 25, 2017, https://www.publicagenda.org/blogs/dan-yankelovich-honored-for-excellence-in-public-opinion-research.

The Problem of Measuring the Human Factors

Many organizations lack insight into the human factor because they fail to adequately measure state and change in security culture. They may hire consulting services to survey and interview their employees about their security awareness. These exercises tend to be resource-intensive, expensive, and incomplete when it comes to evaluating every employee. The surveys used may be created by specialists who are not social scientists, thereby missing important aspects of human factors. Analyzing the data takes time, and is likely to fail to capture a complete picture of the security culture in the organization the survey is undertaken.

Other enterprises measure the outcomes of their security awareness activities to obtain data for comparison. What organizations decide to track, however, might not provide meaningful/valid information that helps measure change in security culture. These points of analysis could instead yield vanity metrics,[8] a used to describe data which looks good on the surface but does not provide any underlying information about what companies need/want to know. Some examples include employee attendance, completion rates, and content scoring for security awareness seminars.

[8] Eric Ries, "Vanity Metrics vs. Actionable Metrics – Guest Post by Eric Ries," The Tim Ferriss Show, last modified May 19, 2009, accessed October 25, 2017, https://tim.blog/2009/05/19/vanity-metrics-vs-actionable-metrics/.

Measuring Culture Requires a Scientific Approach

Organizations can adequately measure change in their security culture only via a scientific approach. To be effective, the method must holistically address numerous elements of security culture. A scientific approach must address on the basis of a synthesis of the scientific definitions of the seven dimensions of culture: attitudes, cognition, behavior, commitment, norms, responsibilities, and compliance. It must then leverage these elements as a cultural context from which organizations can analyze their security culture, including all information and communication tools used by employees.

One such approach that scientifically measures security culture is the CLTRe Toolkit. It is a software-as-a-service (SaaS) platform that allows organizations to assess, build, and improve their security culture.[9] The tool is built upon the Security Culture Framework, an open structure which companies can use to construct and maintain security cultures.[10]

The CLTRe Toolkit integrates a scientific method of measuring, and a

[9] "The Security CLTRe Toolkit," CLTRe, accessed October 27, 2017, https://get.clt.re/the-cltre-toolkit/.

[10] "Welcome aboard!," The Security Culture Framework, last modified September 4, 2014, accessed October 27, 2017, https://securitycultureframework.net/welcome/.

The seven security culture dimensions

ATTITUDES

Employees’ feelings, thoughts and emotions about the various activities that pertain to security culture.

COGNITION

Employees’ awareness, knowledge and beliefs regarding practices, activities and self-efficacy that are related to security culture.

BEHAVIOR

Actual or intended activities of employees that have direct or indirect impact on security culture and information security, including risk taking behavior.

COMMUNICATION

The way that employees communicate and interact among each other, exchange support regarding security issues, incident reporting

NORMS

Unwritten expectations regarding appropriate behaviors pertaining to usage of information technology in organizational context, perception of what practices are normal and unproblematic.

RESPONSIBILITY

Perceived obligation or role to behave correctly towards maintaining security culture.

COMPLIANCE

Awareness of existing organizational policies on information security, understanding and making significance of them, acting in line with them.

scientific method of prediction. Measuring is based on a rigorous procedure of developing measurement scales as set forth by DeVellis[11]. These steps includes

- the development of a large initial pool of assessment items
- pilot testing
- cross validations
- validity and reliability testing

This approach results in a measurement instrument with high psychometric qualities. The instrument allows organizations to assess the true nature of their security culture and its components, and to compare such assessments within organization across departments/teams and between various organizations, thereby providing a baseline for benchmarking.

The scientific method of prediction is based on advanced statistical algorithms (such as structural equation modeling, multilevel modelling and big data approaches) and allows the CLTRe Toolkit to identify correlations between elements of an organizations' security culture and employee behavior.

We can demonstrate this on the basis of the data collected for the Security Culture Report 2017: the data reveals a moderate influence of norms and behavior. In other words: employees tend to behave more securely when more security-related norms operate on the culture.[12]

The scientific method allows us to compute a formula that includes each of the dimensions of culture.

Collecting data from a large number of employees across industry sec-

[11] DeVellis, R. F. (2003). Scale development: Theory and applications (Vol. 26). Sage publications.

[12] Kai Roer and Gregor Petric, *Indepth insights into the human factor: The 2017 Security Culture Report* (CLTRe North America, Inc., 2017), 64-66.

tors and country borders provides us with empirical evidence of security culture and it’s presence in organizations. The collected data provides an opportunity to further improving the formual by regression analysis to determine item and dimension correlations.

Metrics development

Following a standard and scientifically validated procedure for scale construction (DeVellis, 2003) an initial pool of 101 survey items were developed. On the basis of expert evaluation and pilot testing, a refined set of 45 items was selected. Items were evaluated for clarity, readability, social desirability bias by experts trained in survey design and item development.

Exploratory and confirmatory factor analytical procedures using the R software package were used to confirm the seven-dimension structure of the security culture concept. Additional analyses were performed to confirm discriminatory and convergent validity of security culture concept. Analysis of Cronbach’s alpha on all seven dimensions of security culture proves that the metrics used are internally consistent.

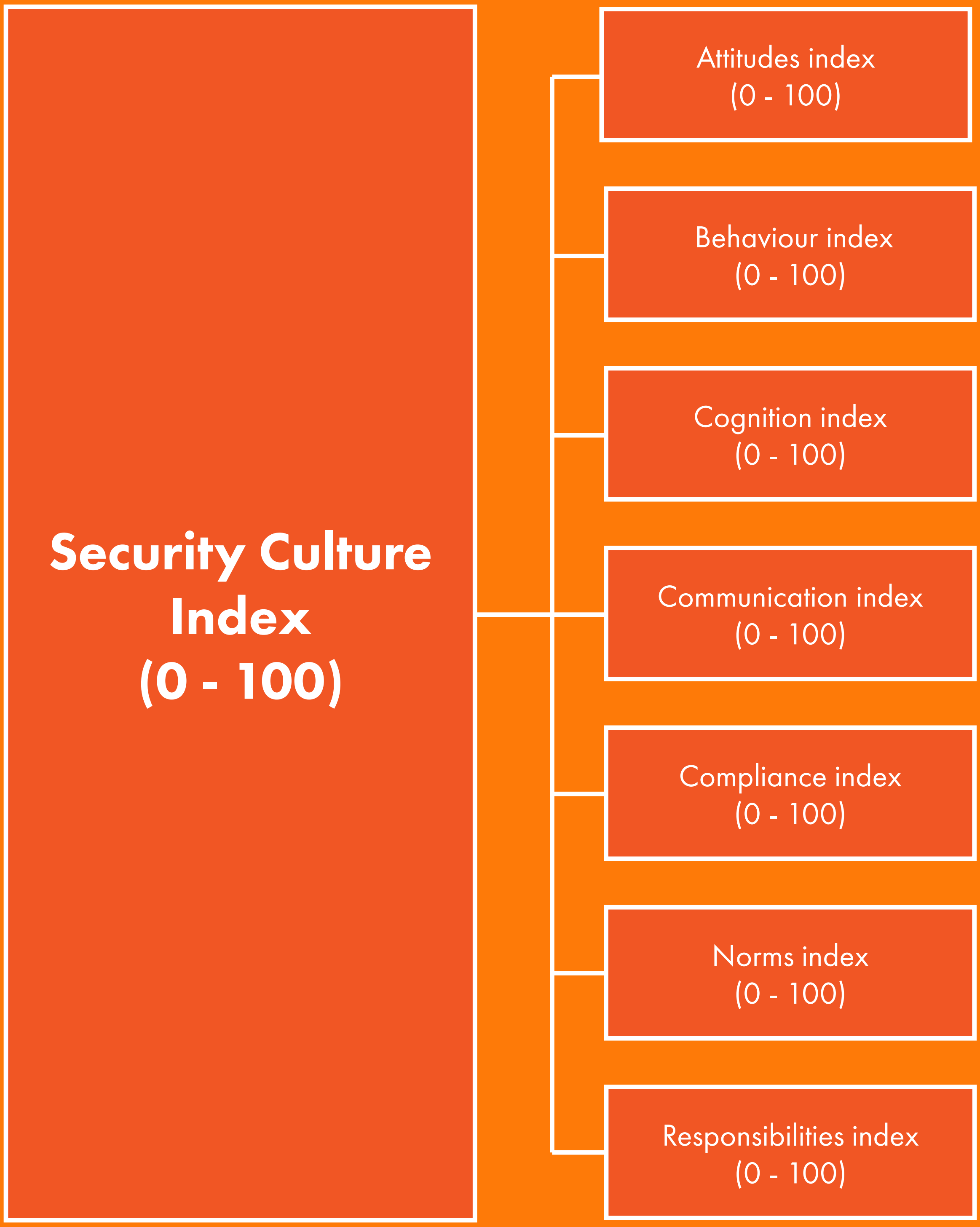
The development of the metrics used in the CLTRe Toolkit followed a strict scientific procedure, which allows us to claim that measures are valid and reliable – in other words, that they are measuring what they intend to measure and are valid instruments for obtaining true (or reasonably accurate) information about reality.

The formula of the security culture index

The formula for measuring security culture draws from research into social science, and can be expressed as follows:

$$\begin{aligned}
\text{Employee behavior} = {} & \\
& \text{Constant} \\
& + \beta 1 * \text{Cognitions} \\
& + \beta 2 * \text{Attitude} \\
& + \beta 3 * \text{Communication} \\
& + \beta 4 * \text{Norms} \\
& + \beta 5 * \text{Responsibility} \\
& + \beta 6 * \text{Compliance} \\
& + \text{Error}
\end{aligned}$$

Each of the dimensions use a 0 to 100 index to produce a security culture index per dimension as well as a total security culture score. The values of the indices range on an interval scale from disastrous security culture (score=0) to optimal security culture (score=100), where higher values represent a higher maturity of security culture or one of its (sub) dimensions.



Security Culture Index (0 - 100)

Attitudes index (0 - 100)

Behaviour index (0 - 100)

Cognition index (0 - 100)

Communication index (0 - 100)

Compliance index (0 - 100)

Norms index (0 - 100)

Responsibilities index (0 - 100)

Are these instruments measuring reality?

In survey-based research, skepticism regarding the honesty of answers is common. This mistrust is amplified when concepts that we are trying to apply metrics to have socially desirable connotations. For example, when asking people about their happiness, there is a tendency to get biased results because people don't answer according the true state of their happiness, but rather provide answers regarding their desires about happiness (since they usually want to be happier than they are and because happiness is a societal and often peer-supported value, not to mention that lack of happiness is socially discouraged).

It can be claimed that many attempts to measure (aspects) of security culture fail to account for this issue. One often cited instrument (DaVeiga, 2008), for example, involves such items as »I know what information security is« or »I know what my responsibilities are regarding information security«. Such items receive responses in which more than 98% of respondents agree, which is of course too good to be true. Statements like these don't measure the true value of knowledge or responsibility, but rather the knowledge or responsibility employees think they need to present. Moreover, such information is useless or even dangerous for decision makers, since it can lead to interventions based on invalid data.

The CLTRe Toolkit and the analysis presented here are based on established mechanisms to avoid the types of biases we just discussed and to measure the true state of security culture (or the best possible approximation of it). In other words, the items that are used for employee assessments in this study are scientifically valid and bias-resistant. The most important mechanism to achieve this is to strictly adhere to the procedures described above. In addition several other mechanisms were employed:

- Detection of employees providing the same pattern of answers and their exclusion from the analysis

- Calculation of minimum timings for assessments based on cognitive psychology experiments (Zhang & Conrad, 2015). Using these minimum timings, »speedsters« were excluded, as it is highly likely that respondents who complete the survey too quickly haven't read the assessments

- Mixing positive and negative statements to check for consistency of assessments

- Development of a pilot study, which was conducted on a small sample to correlate assessments with so called »social desirability items« (Hays et al.1989). Items with significant bias were excluded.

The CLTRe Toolkit

The CLTRe Toolkit consists of a complete set of tools to collect data, analyze the data, report data to different stakeholders, compare and benchmark teams and business units, and to interact and engage the employees and the security team in assessing, building and improving security culture.

With the CLTRe Toolkit, organizations can evaluate the human factors, and therfore the security culture of their entire workforce. They can also obtain more granular details across particular teams and departments, business units, and borders/regions. The CLTRe Toolkit provides a dashboard that can identify the areas of security culture that are particularly weak – either it is communicating security information, compliance, behavior, knowledge, general attitudes of employees, or the lack of security norm adherence.

Book a demo

The CLTRe Toolkit helps organizations measure change in their security culture and distribute assessments and learning activities accordingly. Its formula does not produce vanity metrics; it yields actionable metrics that allow companies to target individual employees, teams, and departments for improvement. As such, it constitutes a scientific approach by which companies can avoid lulling themselves into a false sense of security and instead measurably reduce their organizational risk.

Measuring security culture using the CLTRe Toolkit is recommended practice by the European Union Agency For Network and Information Security[13] and is considered best practice in the Security Culture Framework, the free and open method to build and improve security culture[14].

Contact

Interested parties can book a free demonstration of or request an offer to implement the CLTRe Toolkit. They can do so by contacting sales@clt.re or book a demo at the website https://get.clt.re/

CLTRe AS
Bleikerveien 17, 1387 Asker, Norway
https://get.clt.re/
sales@clt.re

[13] ENISA, *Cyber Security Culture in organisations* (ENISA, 2018), 19-24.

[14] https://securitycultureframework.net/

Bibliography

Beaver, Kevin. “Make Security Culture Your Top Priority.” Security Intelligence. Last modified October 16, 2017. Accessed October 18, 2017. https://securityintelligence.com/make-security-culture-your-top-priority/.

CLTRe . “The Security CLTRe Toolkit.” Accessed October 27, 2017. https://get.clt.re/the-cltre-toolkit/.

Da Veiga, A. (2008). Cultivating and assessing information security culture (Doctoral dissertation, University of Pretoria).

DeVellis, R. F. (2003). Scale development: Theory and applications (Vol. 26). Sage publications.

Fahey, Ryan. “Security Awareness -- Definition, History, And Types.” Infosec Institute. Accessed October 20, 2017. http://resources.infosecinstitute.com/category/enterprise/securityawareness/.

Friedman, Will. “Dan Yankelovich Honored for Excellence in Public Opinion Research.” Public Agenda. Last modified November 19, 2015. Accessed October 25, 2017. https://www.publicagenda.org/blogs/dan-yankelovich-honored-for-excellence-in-public-opinion-research.

Hays, R. D., Hayashi, T., & Stewart, A. L. (1989). A five-item measure of socially desirable response set. Educational and Psychological Measurement, 49, 629-636.

Kaspersky Lab. “The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within.” Accessed October 24, 2017. https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

Mind Tools. “The Seven Dimensions of Culture.” Accessed October 23, 2017. https://www.mindtools.com/pages/article/seven-dimensions.htm.

Ponemon Institute LLC. “Managing Insider Risk through Training and Culture.” Published May 2016. Accessed October 20, 2017. https://www.experian.com/assets/data-breach/white-papers/experian-2016-ponemon-insider-risk-report.pdf.

Ries, Eric. “Vanity Metrics vs. Actionable Metrics – Guest Post by Eric Ries.” The Tim Ferriss Show. Last modified May 19, 2009. Accessed October 25, 2017. https://tim.blog/2009/05/19/vanity-metrics-vs-actionable-metrics/.

Roer, Kai, and Gregor Petric. Indepth insights into the human factor: The 2017 Security Culture Report. CLTRe North America, Inc., 2017.

Rouse, Margaret. “security awareness training.” TechTarget. Last modified November 2011. Accessed October 23, 2017. http://searchsecurity.techtarget.com/definition/security-awareness-training.

SecureDataService. “Article 32, EU GDPR, ‘Security of processing.’” Accessed October 23. 2017, https://www.privacy-regulation.eu/en/32.htm.

SecureDataService. “Article 47, EU GDPR, Binding corporate rules.’” Accessed October 24, 2017. https://www.privacy-regulation.eu/en/47.htm.

The Security Culture Framework. “Definition of Security Culture.” Last modified September 4, 2014. Accessed October 18, 2017. https://securitycultureframework.net/definition-of-security-culture/.

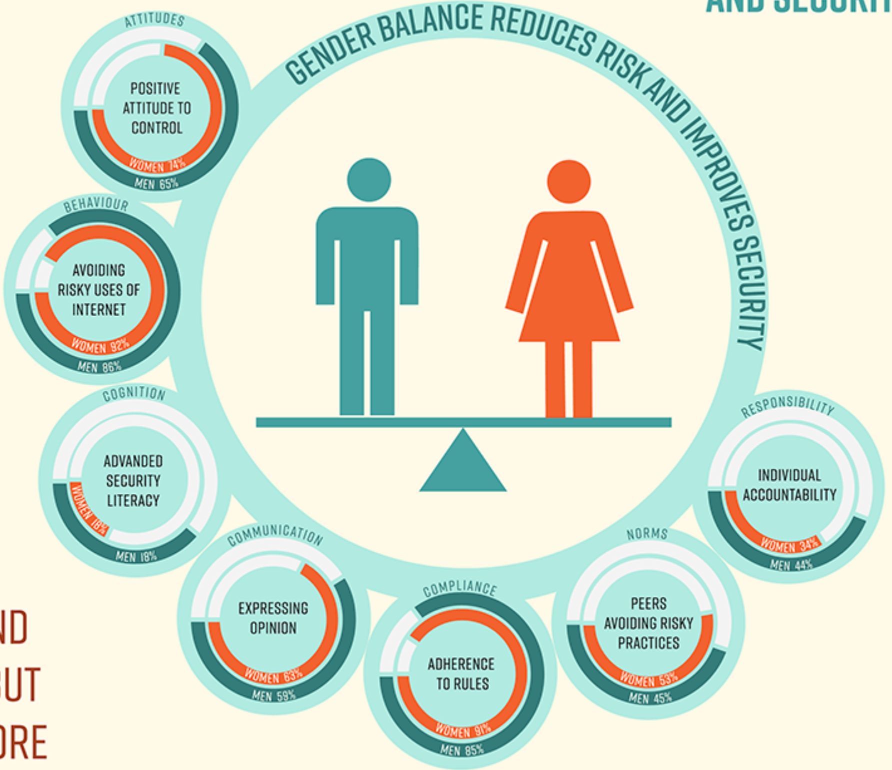
The Security Culture Framework. “Welcome aboard!” Last modified September 4, 2014. Accessed October 27, 2017. https://securitycultureframework.net/welcome/.

Zhang, C., & Conrad, F. (2014, July). Speeding in web surveys: The tendency to answer very fast and its association with straightlining. In Survey Research Methods (Vol. 8, No. 2, pp. 127-135).

Zorz, Zeljka. “Security awareness is good, but good security culture is better.” Help Net Security. Last modified May 8, 2017. Accessed October 23, 2017. https://www.helpnetsecurity.com/2017/05/08/build-security-culture/.

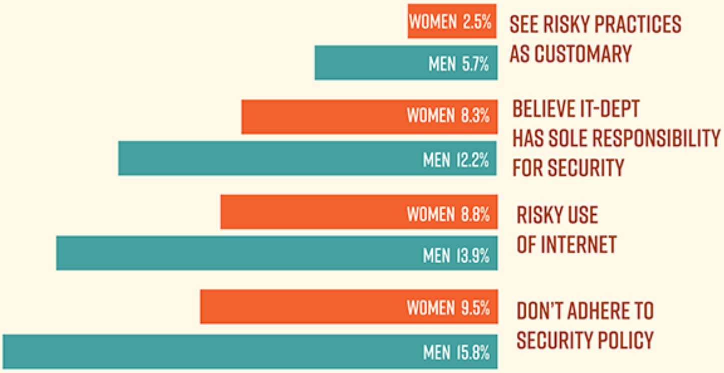
CLTRe GENDER MATTERS

GENDER, RISK, AND SECURITY



MEN REPORT THAT THEY UNDERSTAND SECURITY BUT DISPLAY MORE RISKY BEHAVIOUR

WOMEN REPORT LOWER UNDERSTANDING BUT HAVE HIGHER ACCEPTANCE FOR RULES AND BETTER SECURITY BEHAVIOUR



A whitepaper by CLTRe AS - https://get.clt.re

Contact

CLTRe AS
Bleikerveien 17, 1387 Asker, Norway
https://get.clt.re/
sales@clt.re

Co-funded by the Horizon 2020 programme
of the European Union

Recommended by ENISA