Cybersecurity Awareness Study 2020

More attention and safety

www.lucysecurity.com
www.lucysecurity.com/laws

Lucy

CONTENT

05
INTRODUCTION

06
KEY FINDINGS

08
RESULTS IN DETAIL

- *Business Benefits and Cybersecurity Awareness*
- *Challenges*
- *Use of Cybersecutity Awareness*
- *Corporate Security and Cybersecurity Awareness*
- *Cybersecurity Awareness and Security Strategy*

18
CONCLUSION

19
FIGURES AND TABLES

25
METHODOLOGY

26
FOOTNOTES AND RESOURCES

27
CONTACTS BY REGION

The benefits of Cyber Security Awareness go much further than 'just' better trained employees and fewer security incidents.

– Palo Stacho
Head of LUCY Security

INTRODUCTION

The usefulness of Cybersecurity Awareness, especially of phishing simulations, is currently widely discussed in the public domain. Media coverage of enterprise hack attacks and data leakage has become part of everyday life.

Cyber criminals are acutely focused on the so-called 'human factor'. 97% of Internet attacks are aimed at people. Only three percent are directed against systems [1]. Furthermore, it is a fact that 91% of successful attacks are triggered by careless employees [2].

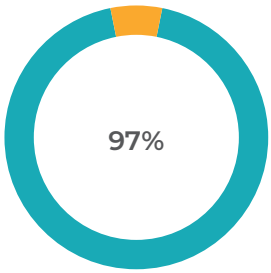
More and more organizations are becoming aware of this fact. Not only large corporations but medium-sized and small businesses (SMEs) as well are investing increasingly both in professional IT security solutions and in the training of their employees to make them more security-conscious.

21st century employees need to know which current threat scenarios come from the Internet and must be able to recognize potential attacks. In addition to classic IT security based on hardware and systems, cyber security awareness strives for the general protection of the organization from the damages of cybercrime. This is implemented through specific training of the employees. Tools are also made available to employees, encouraging them to report suspicious e-mails and have them investigated. Through internal analyses, Lucy Security has determined that correctly implemented awareness programs increase a company's security by up to ten times.

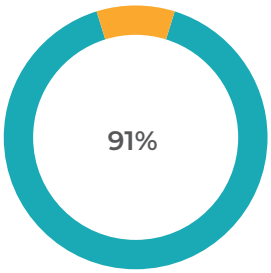
However, the benefits go much further. Although previous studies have focused more on technical aspects of cybersecurity awareness and on strengthening IT security, the present study "Benefits and Challenges of Cybersecurity Awareness 2020" also explores the overarching company-wide benefit potential.

This report shows that the impact of cybersecurity awareness is more diverse than expected. The impact goes beyond 'just' better trained employees or fewer security incidents. There are also positive effects on the corporate culture and the working atmosphere of the companies surveyed. It becomes apparent that the challenges are not only of a technical nature or due to insufficient budget, but that awareness often poses increased challenges to the management and is clearly an innovation task. Ultimately, the goal is to achieve safe employee behaviour among the workforce.

Effective and sustainable Cybersecurity Awareness affects every company! The implementation has never been easier than today, when a considerable number of solutions are available on the market. When using such products and platforms, it should be kept in mind that integrated suites should be used wherever possible. And since security is more of a process than a product [3], special attention is paid to costs. Awareness measures are now part of everyday work and must be carried out continuously. If the implementation is complicated or too expensive, the security of the company will be impaired.



> of the Attacks try to trick a user with some social engineering scheme



> of Cyberattacks and the resulting data breach begin with a spear pishing email

KEY FINDINGS 2020

Almost all of the organizations surveyed have implemented cybersecurity awareness measures (96%) and four out of five companies conduct special phishing simulations.

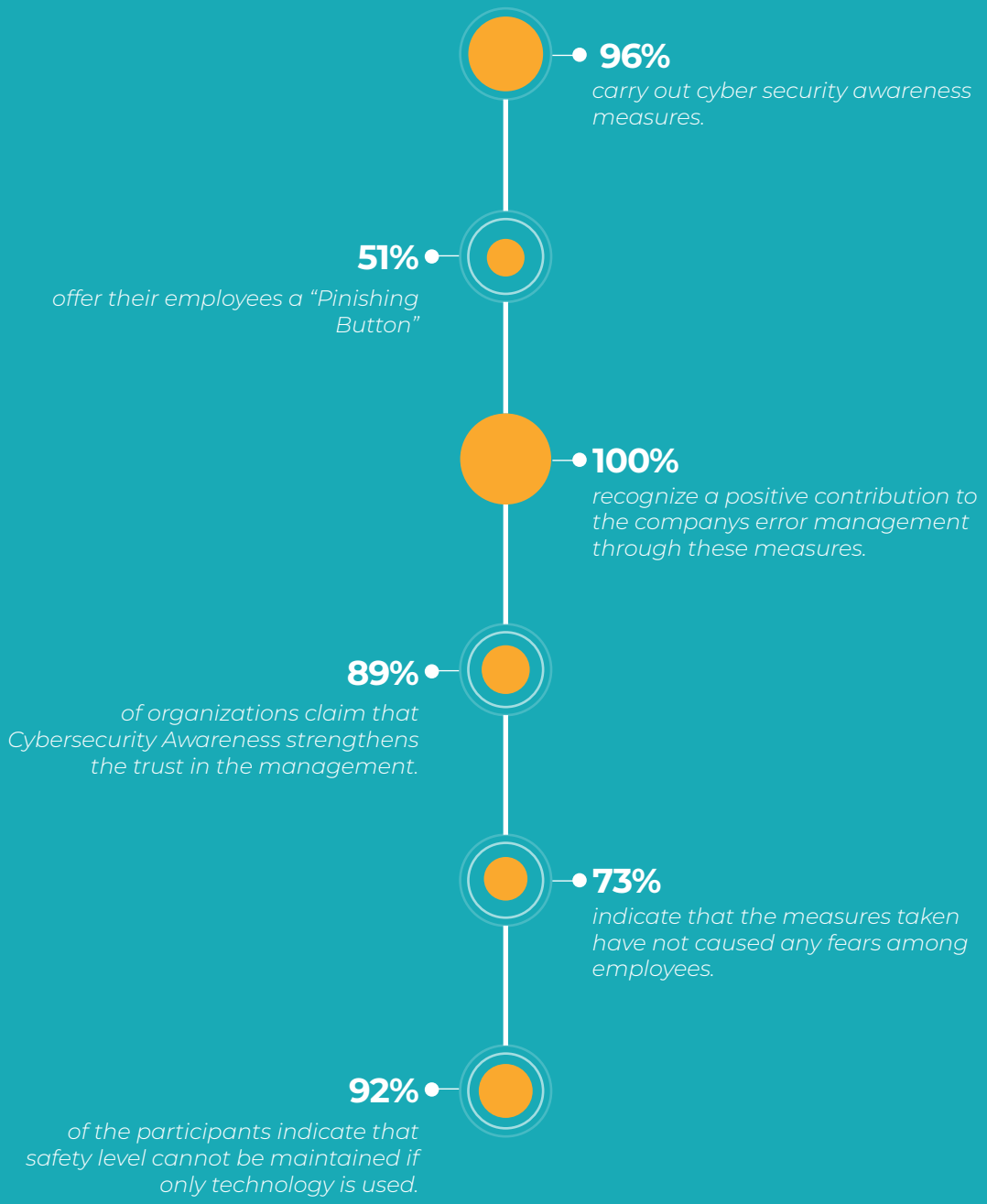
This result is not surprising, considering the international target group of around 900 IT security professionals. However, it is noteworthy that only slightly more than half of the organizations include their employees in their security measures: Only 51% of the companies have a 'Phishing Incident Button' in place. On the one hand these buttons activate the 'human firewall' and on the other hand they provide the insecure employee with a simple but powerful tool that offers great support in the daily handling of emails.

Cybersecurity Awareness has an overall benefit for the company that goes far beyond IT security: All (!) respondents of the study claim that Security Awareness has a positive effect on the error management culture of the company. Furthermore, 89% of the organizations state that the measures have strengthened the trust in the management. This means that there is a very high level of acceptance for security awareness among employees in the companies and that management should do something right and useful here. It is therefore not surprising that almost three quarters of the companies' state that the awareness measures implemented do not cause fear among their employees.

The above results lead to the conclusion that cybersecurity awareness significantly contributes to overall corporate security and generates direct positive effects on the working atmosphere and corporate culture. It is therefore only right and of strategic importance that 92% of the study participants state that security levels cannot be maintained if only technical security measures are implemented without security awareness. The often used ISO standards [4] or the NIST framework [5] do not go far enough in the area of awareness. A prominent anchoring of cybersecurity awareness in every organization's IT strategy is therefore a must!

No topic is without challenges: the biggest challenges are achieving user acceptance, lack of resources (personnel, time, and money) and ensuring broad coverage of the employee base. This list is followed by a lack of management support, ensuring effectiveness and the challenge of managing change.

KEY FINDINGS AT A GLANCE



Source: LUCY Cybersecurity Awareness Survey 2020

RESULTS IN DETAIL

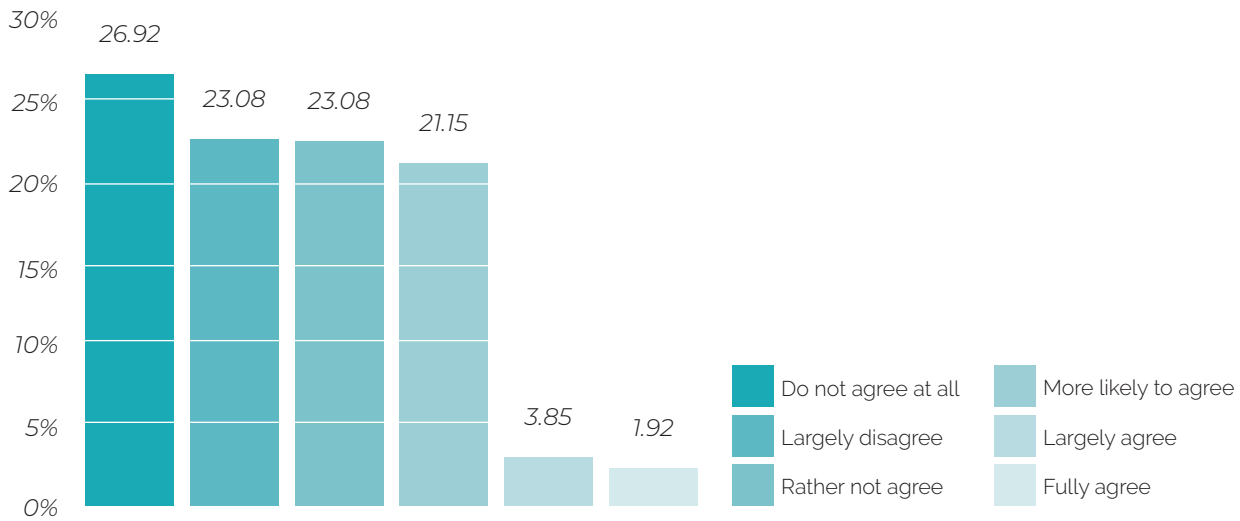
The results of the survey speak for themselves: The positive contribution of Cybersecurity Awareness goes beyond improving general corporate security:

The results of the survey speak for themselves: The positive contribution of Cybersecurity Awareness goes beyond improving general corporate security:

- *In all (100%) companies, cybersecurity awareness leads to improved error culture.*
- *95% of the organizations were able to improve the working atmosphere with security awareness.*
- *89% state that awareness measures have strengthened trust in the management.*
- *73% state that the awareness measures did not cause fear among the staff.*

With almost three-quarters of the responses being 'no', the assumption that cybersecurity awareness measures trigger fears among employees has been refuted. However, the fact that a relevant proportion of 27% of responses indicate anxiety among the workforce deserves closer examination: the data show that the fears that arose among organizations were largely moderate in nature. Only just under 6% of the answers show a rather high rating in terms of triggering anxiety.

The security awareness measures have triggered fears among the workface

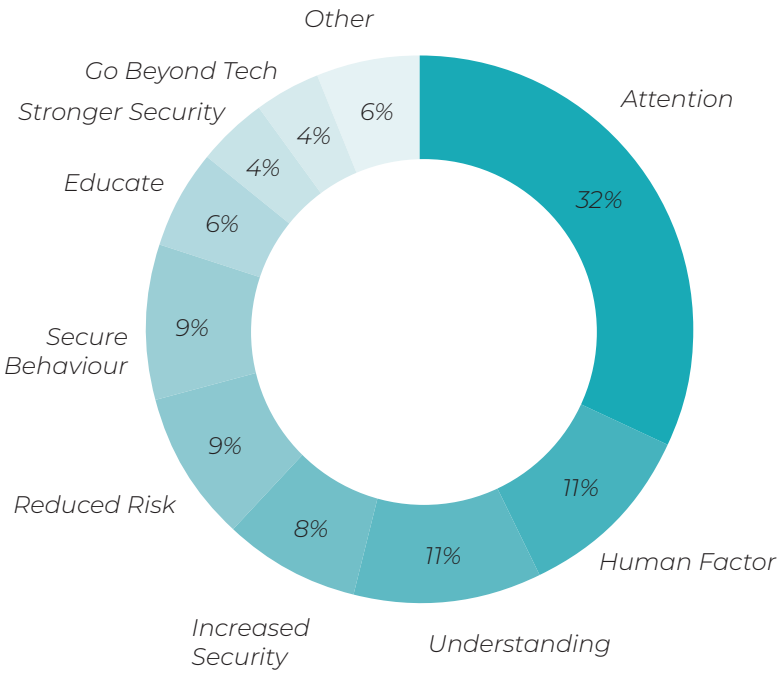


Source: LUCY Cybersecurity Awareness Survey 2020

Major Benefits with Cybersecurity Awareness

ANALYSIS

The evaluation of the free responses for individual benefit brought to light various thematic clusters. Almost one third of the organizations mention the maintenance of alertness as the top benefit (32%). This is followed by the activation of the 'human factor' with 11%. This means the integration and commitment of the employee in the alarm chain of the company in case of potential security incidents. For another 11%, the primary benefit is the employees' understanding of cyber risks. Other relevant benefit clusters are: Increased IT security, respectively lower security risks, achieving safe online behavior by the employees, the training of the employees, a stronger IT security posture or measures that start where the technology ends (with people). In the following, some selected answers to the question "What is, in your opinion, the greatest benefit of Cybersecurity Awareness?"



Source: LUCY Cybersecurity Awareness Survey 2020

HUMAN FACTOR CLUSTER

- *"The weakest factor in the chain of measures - the human being - is strengthened.*
- *"Capacity utilization, utilization of employees."*
- *"The human factor, attention is improved and the scope for attack is reduced."*

UNDERSTANDING CLUSTERS

- *"Employees' understanding of information security."*
- *"Awareness of colleagues that cyber-attacks exist and how to react correctly when you are affected."*
- *"Awareness that it is always possible to be phished."*

ANDERE (OTHER)

- *"Security becomes visible!"*
- *"Fewer incidents, integration of employees."*
- *"Simplified procedure through the availability of many templates."*

CHALLENGES

When it comes to the implementation of cybersecurity awareness measures, there are three classes of challenges.

TOP CLASS

The top class includes the battle for **user acceptance, the struggle for resources (budget, time) and the achievement of reach.** Reach refers to the effort to reach and influence as many colleagues as possible.

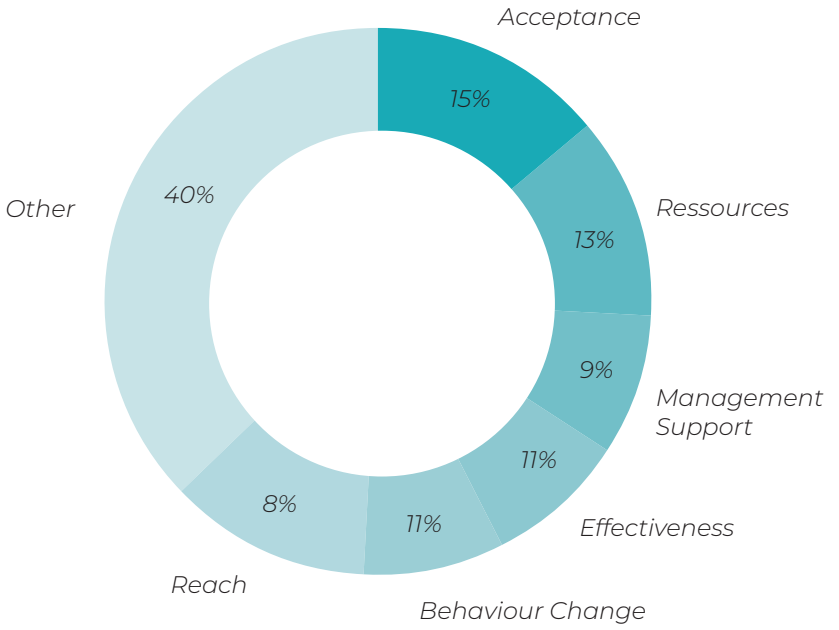
SECOND CLASS

The second class of challenges is obtaining management support, effective implementation and managing the desired change. Effectiveness is mainly about the right design of the training offer, to ensure that the necessary topics are taught in a targeted and recipient-oriented manner or that the topic remains relevant to the employees in the long term. In managing the change - the Behavioural Change amongst the workforce towards the safe behaviour of each individual employee - challenges such as the length of the process are involved. In addition, aspects such as the motivation of indifferent employees and dealing with the ignorance of employees are also mentioned.

THIRD CLASS

The third class includes all other challenges of various kinds. Below are selected answers to the question “What do you consider to be the biggest challenge of Cybersecurity Awareness?

Major Challenges with Cybersecurity Awareness



Source: LUCY Cybersecurity Awareness Survey 2020

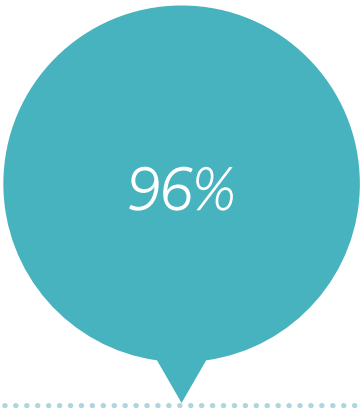
ANSWERS TO THE CLASS 'Other':

- *"Stay close to reality because hackers don't follow any rules."*
- *"Adapting to actual threats."*
- *"The bad guys just keep getting better."*
- *"build awareness into the daily work of your employees."*
- *"Ensure that employees don't become dulled with varied campaigns."*
- *"The human being / employee is often the weakest link in the chain, cyber-attacks are getting stronger and stronger. The number is increasing and the attacks are becoming more sophisticated.*
- *"Keeping sensitivity high and active."*
- *"Getting employees to participate 'voluntarily' in training courses etc."*
- *"Highlighting the usefulness and fighting against' what makes the firewall'.*
- *"Solutions have to be customized, because the offers "off the shelf" are not well prepared.*
- *"That too many simulations are performed."*
- *"Constant balancing between reality and practicability (of campaigns and scenarios)."*
- *"The precision of the tests and the regularity of the tests."*
- *"The filtering and segmentation by user group or class."*
- *"That employees do not have time or little time is allocated for training."*
- *"To train the weakest people (top worst)."*

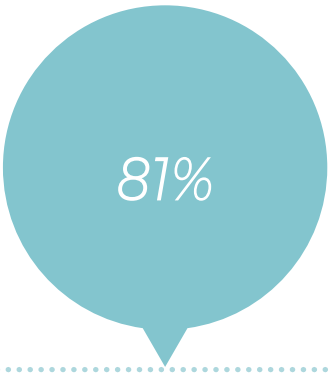
USE OF CYBERSECURITY AWARENESS

The study has confirmed the findings on the fundamental relevance of security awareness that are recognized in the market:

It is worth noting that almost half of the organizations do not include the employee in their security plan: 49% of the respondents do not have a 'Phishing Button' in place. These companies do not exploit the full potential of their staff. The 'Human Firewall' is not activated. On top of that, the Phishing Alarm button is a useful help, especially for employees who are confronted with suspicious messages in their daily work and are uncertain about their legitimacy. Such a "Phish Button" offers a great support in such situations.



of all surveyed organizations conduct awareness training



of all surveyed organizations conduct phishing simulations

Source: LUCY Cybersecurity Awareness Survey 2020

The absence of a Phishing Incident Button results in the loss of much protection potential and user motivation".

– Palo Stacho Head of Studies
LUCY Security AG

60%

of the surveyed organizations use LUCY software

51%

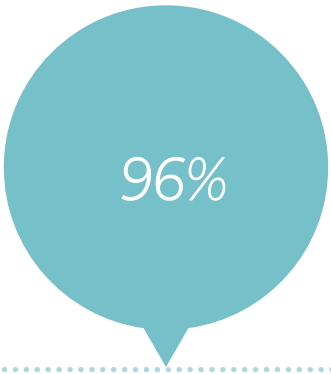
of organizations have a 'Phishing Alarm Button' in place

CORPORATE SECURITY AND CYBERSECURITY AWARENESS

CORPORATE SECURITY

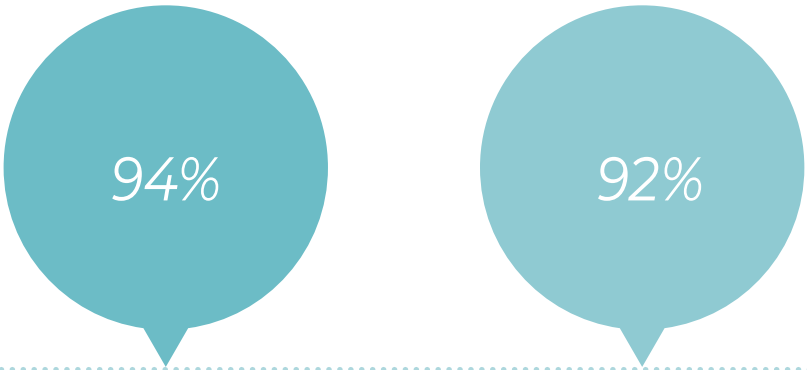
Evidence confirms that Cybersecurity Awareness training increases awareness and contributes to corporate security. At the same time, it refutes claims that phishing simulations weaken the security infrastructure because so-called whitelistings [6] and the like have to be set up for implementation.

are convinced that security awareness measures make real attacks more difficult.



of all organizations state that security awareness leads to a higher level of security.

Source: LUCY Cybersecurity Awareness Survey 2020



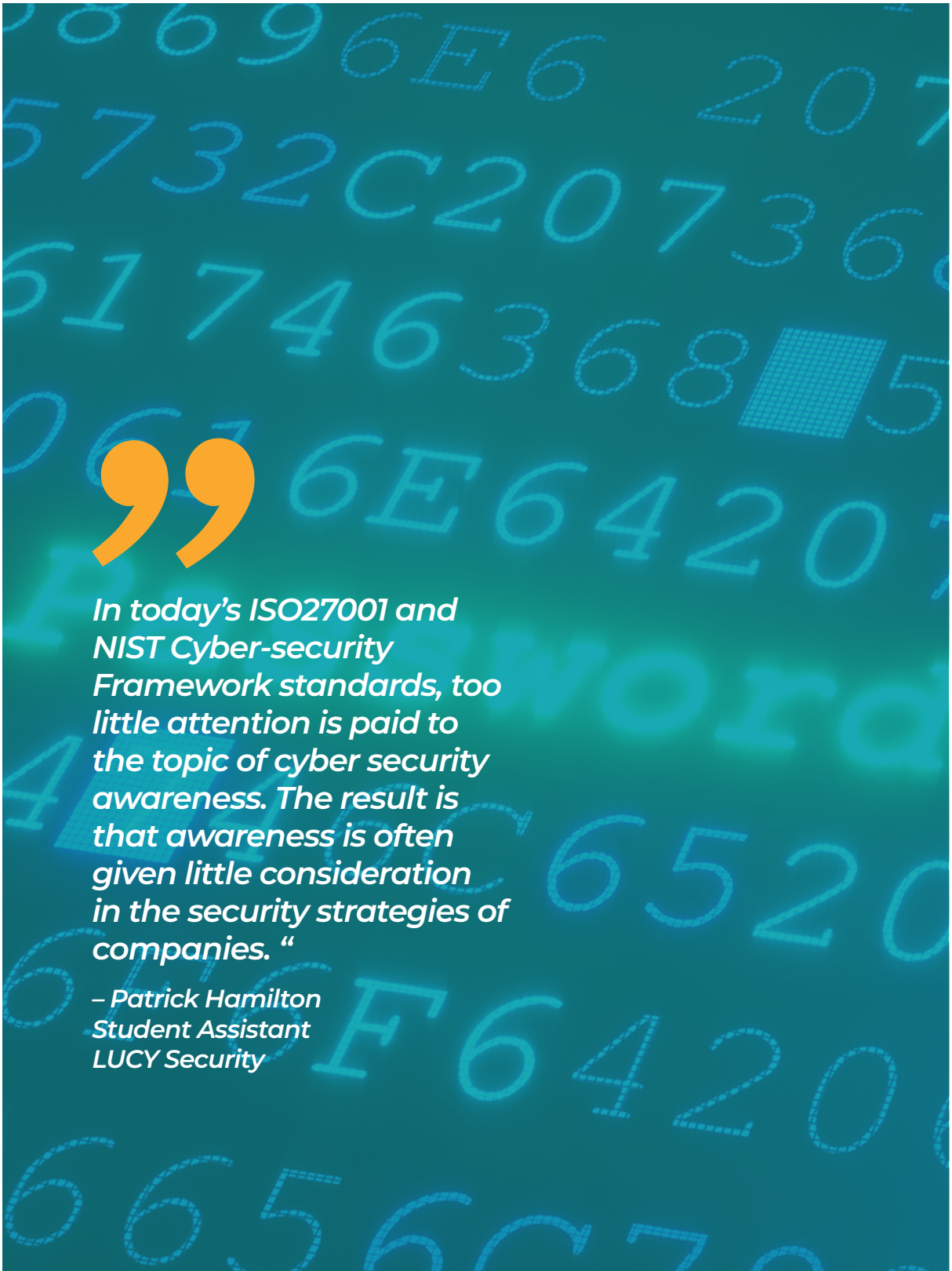
say that cyber security awareness does NOT weaken the IT security infrastructure.

state that security awareness has increased among them.

CYBERSECURITY AWARENESS AND SECURITY STRATEGY

92% of organizations believe that security levels cannot be maintained by implementing only technical security measures

The industrialization of cybercrime and its spread is a phenomenon that is much more recent than most of the security policies and IT strategies currently used in companies. Of course, such policies and strategies are usually updated on an ongoing basis. But the point is that the standards on which such policies are based are revised much less frequently. The last revision of the ISO27001 policy dates back to the year 2013 [4]. Another relevant framework, the NIST Cybersecurity Framework 1.1 is much more recent, i. e. from 2018, but unfortunately even this relatively recent standard has been overtaken by reality. Just by the interim introduction of GDPR [7] and CCPA [8] these standards, from an awareness perspective, are no longer up to date. This is especially true for companies that operate critical infrastructures. Today's recognized standards, ISO27001 and NIST Cybersecurity Framework 1.1, do not adequately address the need for cybersecurity awareness. As a result, the topic of cybersecurity awareness is (still) in the shadow of many corporate IT security strategies.
Cybersecurity Awareness plays an important role in information security and enterprise protection. Without awareness and sensitized employees, organizations are less secure. Awareness training and phishing simulations must be anchored in the security strategy.



In today's ISO27001 and NIST Cyber-security Framework standards, too little attention is paid to the topic of cyber security awareness. The result is that awareness is often given little consideration in the security strategies of companies. "

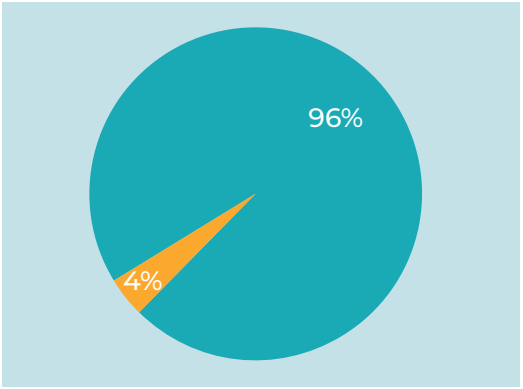
– Patrick Hamilton
Student Assistant
LUCY Security

CONCLUSION

91% of successful Internet attacks start with the employee. Cybersecurity Awareness measures are aimed precisely at this same point - at people. The study shows that companies deploying Cybersecurity Awareness training achieve increased resilience to cybercrime and enhanced IT security.

Without ongoing Cybersecurity Awareness Programs [9] a company has a lower security level than with awareness training and phishing simulations. In 2020, only half of those surveyed use a Phishing Incident Button, which means a waste of employee commitment and hence lost protection potential. All study participants report an improvement in error management culture and 95% confirm a better working atmosphere thanks to cybersecurity awareness. Cybersecurity Awareness measures strengthen the trust in the management. The greatest benefit is seen in security, attention, strengthening the human factor and the understanding of cybersecurity and Internet threats. The biggest challenges are achieving user acceptance, lack of resources (personnel, time, money) and ensuring coverage. This is followed by ensuring management support, effectiveness issues and the challenge to manage change. Phishing simulations and awareness training must be anchored in the IT security strategy. And not to be underestimated: Cybersecurity Awareness makes information security and the efforts around it visible within the company.

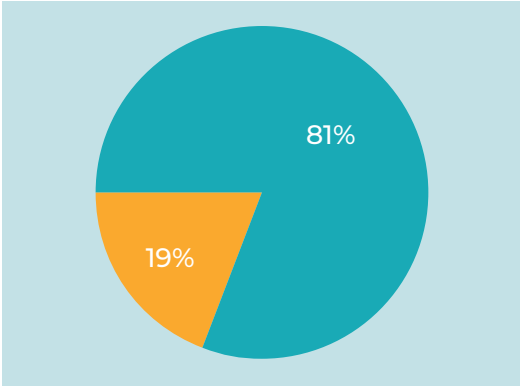
FIGURES AND TABLES



Our organization conducts awareness training.

96% Yes
4% No

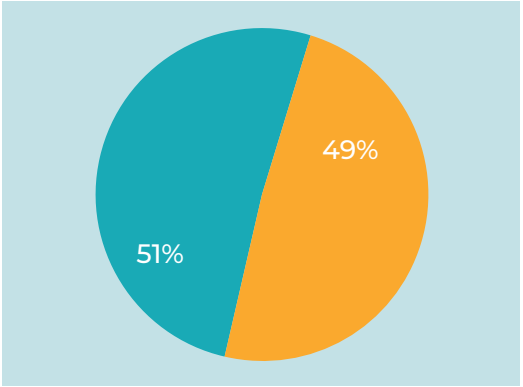
Source: LUCY Cybersecurity Awareness Survey 2020



Our organization carries out pushing simulations.

81% Yes
19% No

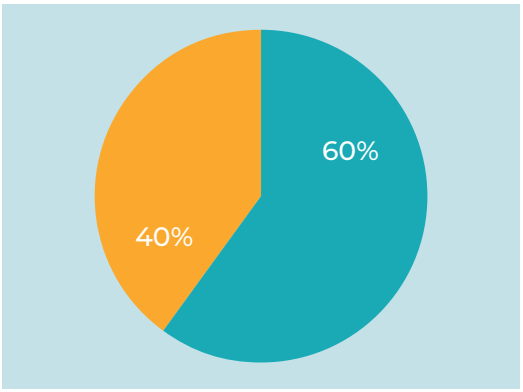
Source: LUCY Cybersecurity Awareness Survey 2020



Our organization provides our employees with a Phishing Button

51% Yes
49% No

Source: LUCY Cybersecurity Awareness Survey 2020

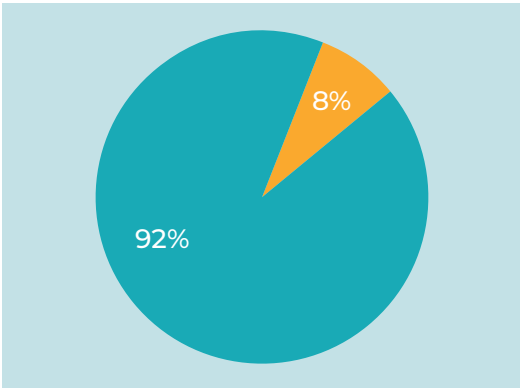


Our organization uses LUCY Software for Cyber Security Awareness

60% Yes

40% No

Source: LUCY Cybersecurity Awareness Survey 2020



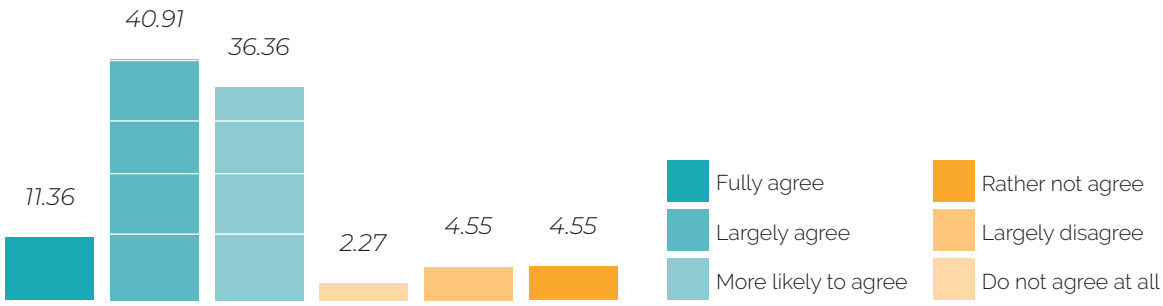
Die Cyber Security Awareness has increased in our organization in the last years/months (i.e. the level of sensitization of the employees)

92% Agree

8% Disagree

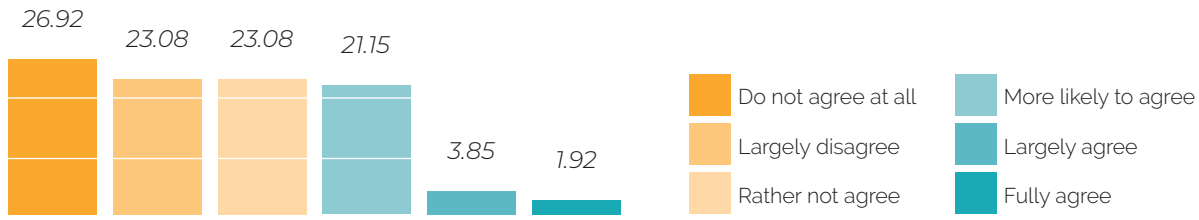
Source: LUCY Cybersecurity Awareness Survey 2020

Trust in the management was improved by the security awareness measures implemented



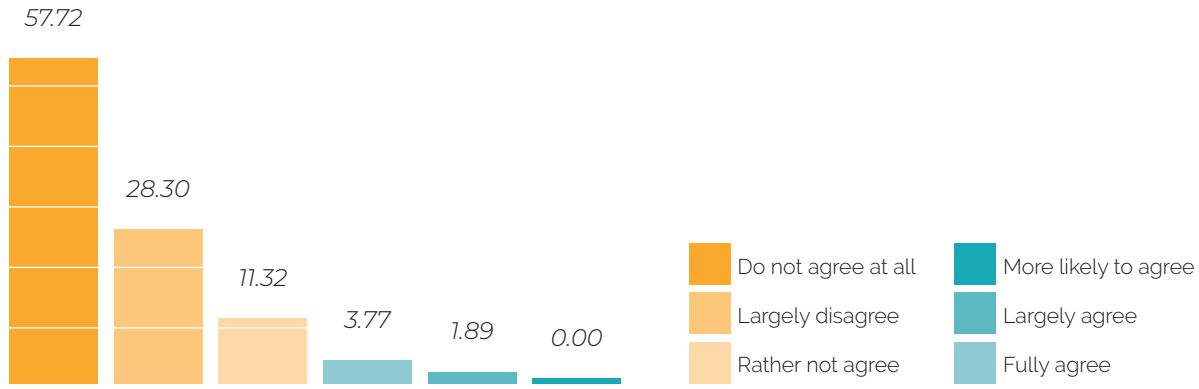
Source: LUCY Cybersecurity Awareness Survey 2020

The security awareness measures have triggered fears among the workforce



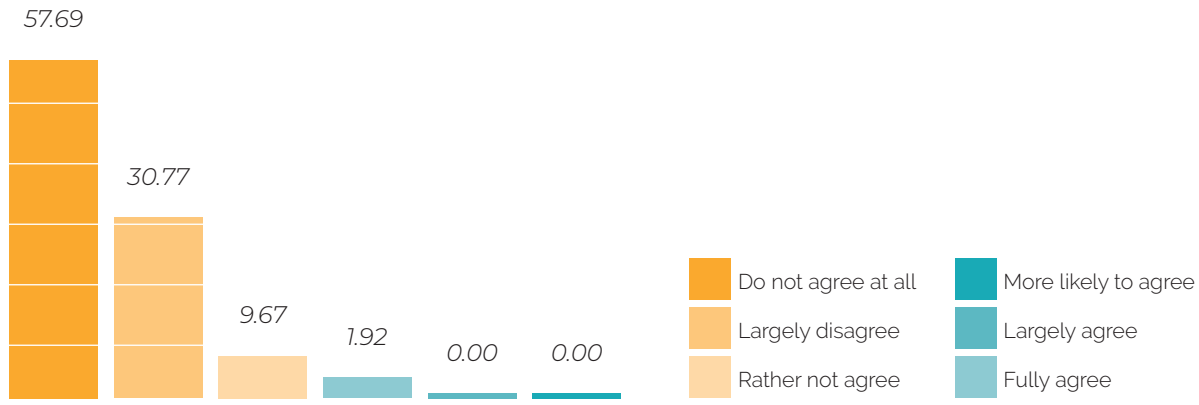
Source: LUCY Cyber Security Awareness Survey 2020

The security awareness measures weaken the companys IT security infrastructure (through whitelistings, exceptions, etc)



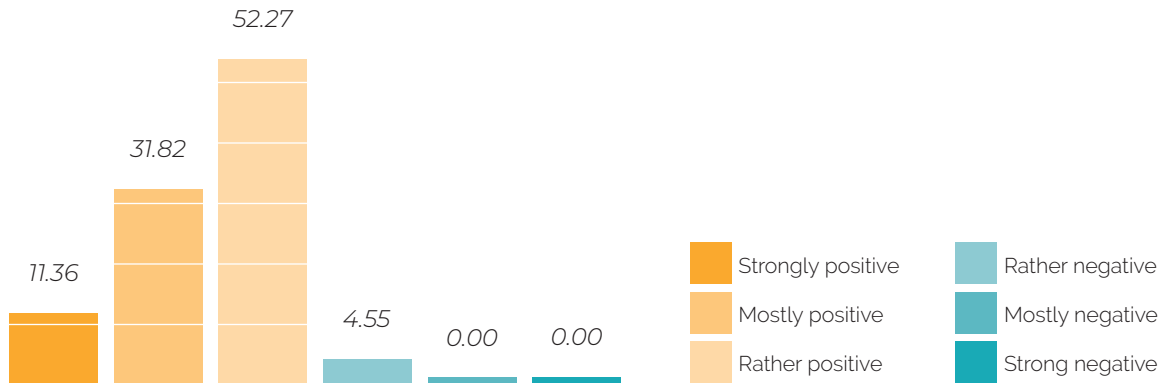
Source: LUCY Cybersecurity Awareness Survey 2020

The security awareness measures make it easier for cyber criminals to carry out malicious hackings attacks (e.g. by using simulation templates for real attacks)



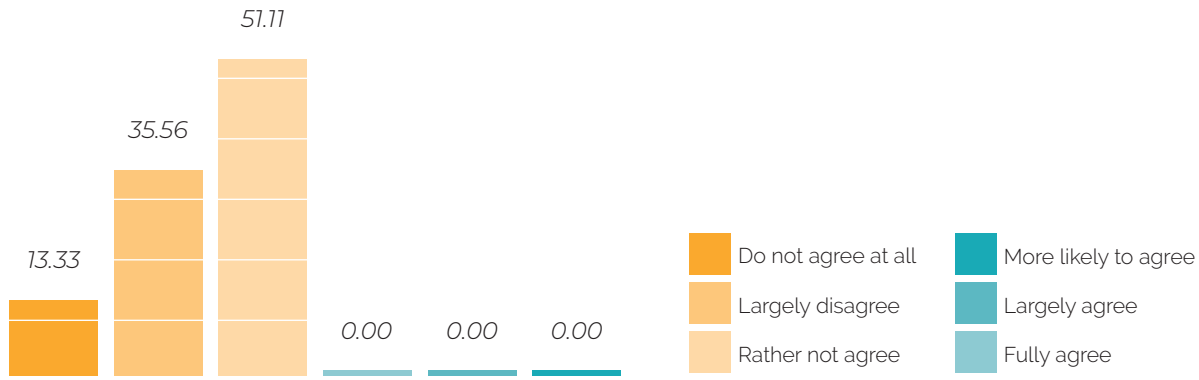
Source: LUCY Cyber Security Awareness Survey 2020

The effects on the working atmosphere through the phishing simulations were



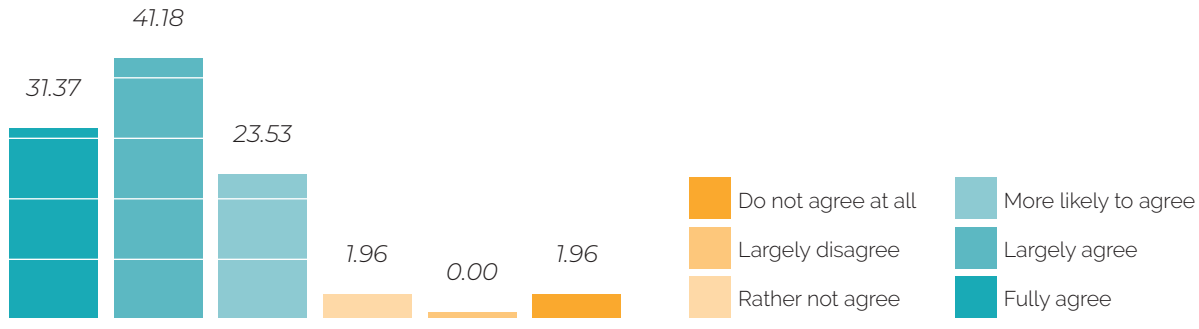
Source: LUCY Cybersecurity Awareness Survey 2020

The influence of the awareness measures had an impact on the culture of errors in the company

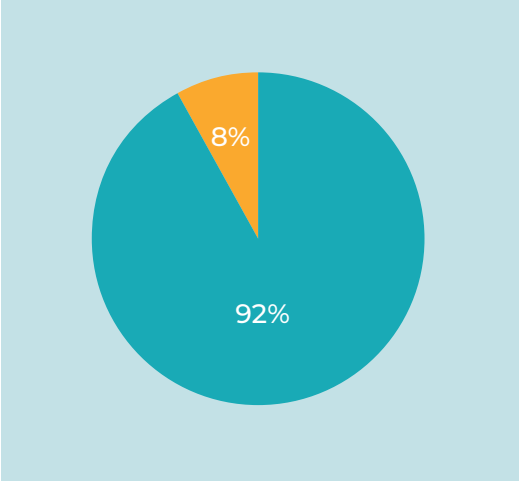


Source: LUCY Cybersecurity Awareness Survey 2020

Security Awareness led to a higher level of security in our organization



Source: LUCY Cybersecurity Awareness Survey 2020



Do you believe that the same level of IT security can be maintained in your organization if the available resouerces and money are invested exclusively in technical security measures (firewalls, application gateways, virus scanners, mail-sandbox systems, etc.)?

8% Yes

92% No

Source: LUCY Cybersecurity Awareness Survey 2020

Survey results for the DACH region

32% of the survey participants come from Germany, Austria and Switzerland. This region shows comparable results with slight differences. Nevertheless, the results are a surprise for the study management: The DACH region itself is more confident about security awareness than the rest of the world!

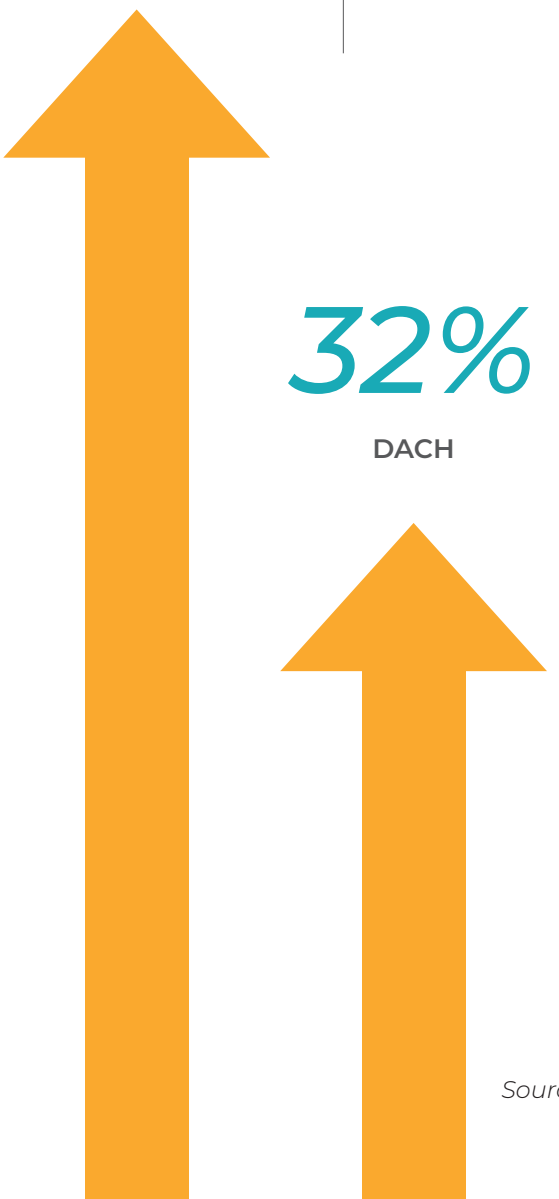
- *In all DACH companies, Cyber Security Awareness improved error management.*
- *91% in DACH state that awareness measures have strengthened trust in the management.*
- *76% in DACH state that the awareness measures did not cause any fears among the employees.*
- *96% of the surveyed DACH organizations conduct awareness training and*
- *83% carry out phishing simulations.*
- *48% of DACH organizations have a 'Phishing Alarm Button' in place.*
- *63% of the DACH-organizations surveyed use LUCY software.*
- *63% of the DACH-organizations surveyed use LUCY software.*
- *90% of the DACH organizations believe that security awareness has increased.*
- *98% of the DACH organizations state that Cyber Security Awareness does NOT weaken the IT security infrastructure.*
- *All DACH survey participants state that Cyber Security Awareness makes real attacks more difficult.*

The above results were a surprise for the study management: The DACH region as a region is is even more convinced of security awareness than the rest of the world!

METHODOLOGY

ONLINE STUDY

The global online study “Benefits and challenges of Cyber Security Awareness 2020” was conducted between June 25 and July 16, 2020 among nearly 900 qualified security specialists. More than 8% of the respondents answered the extensive questionnaire. The proportion of study recipients from the DACH region was 32% of the study recipients. During the same period, the survey was also publicly available and was advertised on LinkedIn [10]. About 12% of all answers have been collected through this channel. Of the respondents, 90% stated that they were security awareness specialists.



Source: LUCY Cybersecurity Awareness Survey 2020

FOOTNOTES AND RESOURCES

01

https://www.knowbe4.com/what-is-social-engineering/

02

https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

03

https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-howprotect-against-phishing

04

https://quotes.thefamouspeople.com/bruce-schneier-939.php

05

ISO27001: https://de.wikipedia.org/wiki/ISO/IEC_27001

06

NIST Cybersecurity Frameworkhttps://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

07

Whitelisting https://en.wikipedia.org/wiki/Whitelisting

08

GDPR https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

09

CCPA – California Consumer Privacy Act -https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

10

Security Awareness Programm: Beispiel SAPF Leitfaden - https://lucysecurity.com/sapf

11

https://www.linkedin.com/feed/update/urn:li:activity:6684493357768552448

CONTACTS

USA & CANADA

Colin Bastable

colin@lucysecurity.com

AFRICA & MIDDLE EAST

Matthias Ernst

matthias@lucysecurity.com

SOUTH EUROPE & LATAM

Eric Naegels

eric@lucysecurity.com

DACH

Palo Stacho

palo@lucysecurity.com

GLOBAL

Oliver Münchow

oliver@lucysecurity.com

www.lucysecurity.com
www.lucysecurity.com/laws

GLOBAL

LUCY SECURITY AG

Chamerstr. 44
6300 Zug
Switzerland

NORTH AMERICA

LUCY SECURITY USA

13785 Research Blvd
Suite 125
Austin, TX 78750