Archives of Business Research – Vol. 13, No. 07
Publication Date: July 20, 2025
DOI:10.14738/abr.1307.19110.
Kartikawangi, D. & Lukas (2025). Advocating Education on Information Security Critical Thinking Using Social Network: A Model. *Archives of Business Research,* 13(07). 32-45.

Advocating Education on Information Security Critical Thinking Using Social Network: A Model

Dorien Kartikawangi
School of Communication,
Atma Jaya Catholic University of Indonesia

Lukas
Faculty of Engineering,
Atma Jaya Catholic University of Indonesia

ABSTRACT

Digital dilemma causes a world of volatility, uncertainty, complexity, and ambiguity (VUCA). This paper aims to explicate the education of users on security-critical thinking in order to prevent and cope with VUCA caused by ICT. In the perspective of engineering, information security is the act of maintaining confidentiality, integrity, and availability of information. Based on this theory, quantitative and qualitative approach is applied with survey and observation for data gathering. Research findings suggest that understanding security is necessary, and communication becomes central in critical thinking advocacy of information security. Here, communication is a form of education in information security critical thinking amplified and disseminated to the public. The quantitative result explains that education background and cohort has unique characteristics on information security in the level of cognitive, affective, and behavioral While qualitative result show that informal education held by NGOs and Government are not specifically focused on critical thinking towards information security, but more general, and delivered massively. Based on these findings, this paper proposes a model of critical thinking in information security education, which consist of three elements: confidentiality, integrity, and availability of information, called ISCT-CIA.

Keywords: communication, ICT, social network, social capital, VUCA

INTRODUCTION

The rapid innovation in information and communication technology (ICT) is enormous and has both positive and negative global impacts. Digital technologies not only support and make the work easier but also raises risks. In this context, an organization as a system influences the digital network society and vice versa, especially in its stakeholders' interaction. There is an information exchange. Information knowledge management facilitates the flow of facts or ideas up and down the chain of command, improve business operations, and contribute to the organization's development. However, a digital dilemma causes a world of volatility, uncertainty, complexity, and ambiguity (VUCA). Previous research on VUCA was mostly done from the organizational management perspective. In this context, ICT is one of the tools to cope with and support organization sustainability. Therefore, understanding the VUCA trend caused by ICT, and research for a solution is important. Preliminary observation research found some evidence that ICT can cause VUCA. Statista (2021) survey on January 2021 reports there are 4.2

billion social media users. Combined with individual direct communication, and aggregating with other communication media, such as WhatsApp, Line, and Telegram shows how different people communicate and maintain relationships compared to previous decades. While in Indonesia, KataData.com (2021) noted that Indonesia's Internet Penetration at the end of March 2021 reached 76.8 percent of the population. Furthermore, Internetworldstats (2021) reported 212.35 million internet users, from the estimated 276.3 million population of Indonesia. Along with conveniences, cost, and time, gained from this communication in this digital era, also emerges risks from the digital technology communication media usage. The massive use of digital technologies is followed by fraud, online scams, intrusion, and data breaches (De', Pandey, & Pal, 2020). In the information technology domain, this is especially called information security. Many issues raised were said related to information security, such as the Cambridge Analytica scandal whose data was improperly obtained from Facebook to build voter profiles, then allegedly influenced voters to act in the 2016 US Presidential poll. Meanwhile, in May 2020, three e-commerce platforms in Indonesia experience data leakage, i.e. 91 million user accounts and 7 million merchant accounts of Tokopedia leaked and sold online on 4 May 2020; then on 5 May 2020,13 million user accounts of Bukalapak were suspected to be leaked; and on 11 May 2020, 1.2 million user accounts of Bhinneka also leaked. Further, in 2021, as reported by the CNN news portal, private data of the President of Indonesia as well as e-HAC were raising issues of conflicts among the responsible parties. Besides, another trend in information security crime called social engineering is increasing in 2022. Social engineering, as an art of deception, is very present in the era of globalization and it intertwines with a plethora of acts of unfair activities (Naumovski and Taneski, 2019). Social engineering, due in part to the increasing popularity and advancements in information technology and ubiquity of devices, has emerged as one of the most challenging cyber security threats in the contemporary age. In the context of cyber security, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal (Aldawood and Skinner, 2018). This situation describes and emphasizes how ICT become a significant contributor to the VUCA world. world.

This paper focuses on elaborating on informal education embedded with formal education that uses the convergence of digital platforms and face-to-face communication to capitalize on social networks. The social network exists before digital, and it becomes broader and more accessible with the support of digital technologies. A social network is an asset for individuals and organizations to gain public support and participation through information exchange. A social network is a social capital, a treasure that can contribute positively to development. Therefore, a model of convergence communication education strategic planning approach is proposed with a focus on information security critical thinking.

LITERATURE REVIEW

A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties. In the digital era, data has become one of the most critical components of an enterprise. Data leakage poses serious threats to organizations, including significant reputational damage and financial losses (Cheng et al, 2017). Furthermore, access to sensitive information such as customers or employee give negative impacts on reputation and leads to financial losses. From the user perspective, the risk of data breaches according to Liu et al (2018) includes 1) hidden correlation between address and location can be used to track

URL: http://doi.org/10.14738/abr.1307.19110

people's possible movement, even the use of public transportations 2) daily data route and possible transportation mode to be used, can be estimated based on the income and private information of the corresponding subject 3) employing artificial intelligence and deep learning, one can mine not only the salary but also other leaked private information pieces. That research explains why private data are so wanted by several parties. Conceptually, social capital and social engineering become the thinking framework. Individuals within the network are called the social network. Researchers found that social network existed even before the digital era and was developed by the coming digital technology. Social networks were understood as an asset that drives the development of capital and contribution to the organization's advancement, which is called social capital. Concurrently, social engineering emerged as the use of information to manipulate human behavior for a specific purpose, namely, utilizing data and digital resources for negative activities taking benefit of human interaction. For example, psychological manipulation to compromise security or sensitive information breach. Philips (2012) explains the interrelationship between social capital and social engineering. Consequently, information security literacy is desperately needed.

Information security as explained by Samonas S and Coss, D (2014) consist of three key elements: confidentiality (C), integrity (I), and availability (A), which are often abbreviated as CIA triad. It ensures the information is secure, despite many challenges or critical situations, such as naturdisasterter, server or network problems, as well as human intentional or unintentional acts. Researchers, such as Bhatt & MacKenzie (2019), and Leaning (2017) remind us that people mostly ignorant about technology, easily become a victim when the stored or transmitted information that was transmitted using digital technology is compromised: loss or data breach, data manipulation, or further become widespread disinformation, causing mild to severe loss.

Responding to data breaches and some security incidents, The Minister of Information and Communication Technology of the Republic of Indonesia (Kominfo, 2019), launched a privacy literacy and digital security in September 2019. This effort was supported by many institutions and claimed to be successful and information security literacy in Indonesia was reported to have significant improvement. This was indicated by the survey conducted by the Global World Digital Competitiveness Index which was released by the Institute Management Development (IMD), ranked 56 out of 63 countries surveyed, quite fall behind, but also improved from the International Telecommunication Union (ITU) rank from 115, now in the position of 111.

Based on the description, this research is searching for the answer of

1. RQ1. The map of digital literacy security and awareness of security risks caused by the use of digital technology
2. RQ2. The education of users on security-critical thinking in order to prevent and cope with VUCA caused by ICT.

RESEARCH DESIGN

The research methodology used is Design-Based Research (DBR) and implements a mixed method. The First step is explorative research done with a descriptive quantitative approach. Atma Jaya Community is stipulated as the population with the accidental sampling technique and the total sample is 108. The data was obtained through the distribution of questionnaires

with a total of 23 statements for the three indicators of information security literacy based on the key elements, namely confidentiality (confidentiality, C), integrity (integrity, I), and availability (availability, A). The validity and reliability test of the measuring instrument refer to Reinard, John C (2006, p. 121) were 0.90 and above is considered highly reliable; 0.80-0.89 consider good reliability; 0.70-0.79 consider Fair Reliability; 0.60-0.69 consider marginal reliability; and under 0.60 is Unacceptable reliability. The calculation of Cronbach's Alpha with the number of 23 statements is 0.805. Thus the measuring instrument has good reliability. While the results of the correlation with the critical value of r, for n = 100, r = 0.197; for n=120, r=0.179, the correlation value is 0.1898. Thus the measuring instrument is declared valid. Furthermore, the data were analyzed by respondent profiles and three elements of information security literacy.

This questionnaire aims to gather digital literacy, especially about data/information security. We will further use the analysis to develop and implement a relevant educational strategy. In this mapping, the following was asked regarding digital communication services

- Cognitive: awareness of the topic
- Affective: views as the user
- Conative: user behavior

And respondent's identity

1. Gender
2. Age range under 20, 20-30, 30-40, 40-50, 50-60, above 60
3. Education: High school, Undergraduate, Master's or Doctorate
4. Occupation: Student, Employee

Table 1: Questionnaire items

Confidentiality	
1.	I trust my data is safely stored on the internet
2.	I trust my data on the internet are well secured
3.	I will tell when someone asks for my email address or phone number
4.	I will ask for the full name and phone number of the person when I meet a new friend/colleague
5.	I will give other people phone numbers only with their respective consent
6.	I will give other people's phone numbers to those who need it
7.	I use easy to remember password
8.	I will tell my personal code to my family/friend
9.	I will tell my password to my family/friend
10.	I save my ID and password in the Google app
11.	I save my ID and Password on my mobile phone
12.	I save my personal photos on my mobile phone
13.	I save my personal ID card (electronic) on my mobile phone
Integrity	
1.	I save important information on my mobile phone
2.	I save my important notes on my laptop
3.	I only trust written information
4.	I record my important data in my notebook
5.	I always confirm/crosscheck any information from trusted sources
6.	I trust information based on the sender

URL: http://doi.org/10.14738/abr.1307.19110

7.	I trust information based on the publisher
Availability	
1.	I always try to keep my mobile phone so that easily contacted
2.	I often contact my friend/colleagues
3.	I back up all my important files at least at two distinct locations and two different media (e.g. flash disk, g-drive/dropbox)
4.	It's okay when I cannot access my data/file due to occasional problems on my device or server
5.	I rely on internet access to support my works
6.	I always hope that I can reliably use the internet to support my works

The first step of research findings is then used as the base to do further research on the role of digital literacy education, especially in the aspect of information security to prevent harm caused by social engineering by other parties who use the information for social capital.

In the second step, based on social capital and digital communication theories, a qualitative approach is applied with participative observation to the information literacy community, which are Tular Nalar, and SiberKreasi. Tular Nalar is a consortium of Ma'arif Institute, Love Frankie, and Turn Back Hoax Community, which support by Google.org. While Siberkreasi is a literacy model that was developed by the Ministry of Communication and Information, Indonesia.

The researcher conducted coding and analysis separately. The final form of such coding is then to be compared and discussed for gaining agreement on the relevant theme of data observed. A summary of such themes is provided in the following sub-paragraphs accompanied by literature reviews of relevant evidence

FINDINGS

The Map of Digital Literacy Security and Awareness of Security Risks Caused by The Use of Digital Technology

Quantitative Data-based Map:

The respondent profile can be seen in Table 1. Based on gender, age and education. The gender of the respondent is female dominant. The age of the respondents in this research are varied, from before 20 to after 60 years old. While education background mostly graduated from high school, vocation, undergraduate, and postgraduate (master and doctorate).

Table 2: Respondents Profile

		N
Gender	Male	45
	Female	63
Age	≤ 20	18
	20-30	48
	31-40	13
	41-50	14
	51-60	9
	≥ 60	6
Education	Highschool	27
	Vocation	5

	Undergraduate	49
	Master	15
	Doctorate	12

The result of the survey shows that there are no significant differences in the three aspects of information security, which are: confidentiality, integrity, and availability, either male or female. Average differences based on gender are relatively small as seen in Table 3. Commonly, people think of security in the sense of secrecy, and therefore Confidentiality (C) aspect, while other aspects such as Integrity (I) and Availability (A) are less understood.

Table 3: Average Scores of Confidentiality, Integrity, and Availability based on gender

Gender	Confidentiality			Integrity			Availability		
	Mean	N	Std. Deviation	Mean	N	Std. Deviation	Mean	N	Std. Deviation
Male	34.9556	45	7.76927	26.5778	45	4.42867	24.2667	45	3.72583
Female	34.2063	63	5.63159	25.3175	63	3.68880	24.4444	63	2.92254
Total	34.5185	108	6.58302	25.8426	108	4.04221	24.3704	108	3.26577

Table 4: Average Scores of Confidentiality, Integrity, and Availability, based on age

Age	Confidentiality			Integrity			Availability		
	Mean	N	Std. Deviation	Mean	N	Std. Deviation	Mean	N	Std. Deviation
≤ 20	34.7778	18	5.49391	25.5556	18	4.39548	23.7222	18	2.84513
20-30	36.0417	48	7.40028	26.1458	48	4.08937	24.2292	48	3.75437
31-40	32.8462	13	4.65199	25.2308	13	5.00256	25.3077	13	2.68901
41-50	32.8571	14	5.61395	25.3571	14	2.70632	23.7857	14	2.32639
51-60	33.4444	9	6.57858	26.2222	9	4.17665	25.5556	9	3.39526
≥ 60	30.6667	6	7.03325	26.1667	6	4.07022	25.0000	6	3.22490
TOTAL	34.5185	108	6.58302	25.8426	108	4.04221	24.3704	108	3.26577

As indicated in Table 4, the highest score on Confidentiality is in the cohort of 20-30 years old age. The Confidentiality scores tend to decrease as the age grows. The steepest decrease is in the cohort of 31-40 years old compared to the previous cohort of the 20s. Also, the case for the cohort above 60 years old compared to an earlier cohort of the 50s. We suspect that the youngster under 20 are very familiar with the technology (digital native) and well educated about its use and its risks. On the other hand, more senior subjects (digital immigrants) focus more on functionality and device usage but not on security concerns.

Average scores of Table 3 do not significantly show differences among the age cohort as well as the three aspects. It can be assumed that all of the subjects are aware of information integrity, and that information is unchanged from the sender to the receiver.

Interestingly, in Table 4, the subjects in the middle, i.e. in the cohort of 31-40 years old, relatively scored the lowest, though the standard deviation is small. It seems that this cohort is more critical of integrity trends and tends to be more concerned about the information integrity they send or receive.

URL: http://doi.org/10.14738/abr.1307.19110

Average scores of Availability based on the subject age as shown in Table 4, indicate that the cohort of 51-60 and 31-40 years old have relatively higher scores than the other, though the difference is not so large. This might relate to the feeling of responsibility to quickly respond and the urge need for always updated information.

The view of Educational background in Table 5, shows that the awareness of information secrecy or Confidentiality scores the highest, compared with Integrity and Availability. It means Confidentiality is the easiest aspect to be understood by all of the subjects. From the education background, highschool-Vocational-Undergraduate students score significantly higher than the Masters and Doctorates (their lecturers)

Table 5: Average Score of C-I-A based on education

Education	Confidentiality			Integrity			Availability		
	Mean	N	Std. Deviation	Mean	N	Std. Deviation	Mean	N	Std. Deviation
Highschool	35.1852	27	7.89370	26.2593	27	4.26608	24.5556	27	4.11688
Vocation	35.0000	5	3.53553	24.4000	5	2.70185	24.0000	5	3.24037
Undergraduate	35.5714	49	5.95819	26.0000	49	3.61132	24.2653	49	2.95646
Master	32.8667	15	6.71743	25.9333	15	5.31126	24.9333	15	3.05817
Doctorate	30.5833	12	5.53433	24.7500	12	4.20227	23.8333	12	2.97973
Total	34.5185	108	6.58302	25.8426	108	4.04221	24.3704	108	3.26577

Table 5 is attractive because it shows the average score for all subjects with a relatively similar understanding of the integrity aspect of the information. Scores were slightly higher for students (high school graduates) and employees (undergraduates). As shown in Table 5. the average score for the Availability aspect is relatively the same for all subjects, there is no significant difference between the four-five education groups. The relatively low value for this aspect means that this aspect is not considered important to pay attention to.

Table 6: Average Score of *C-I-A* based on position

Position	Confidentiality			Integrity			Availability		
	Mean	N	Std. Deviation	Mean	N	Std. Deviation	Mean	N	Std. Deviation
Staff	33.3269	52	6.89336	25.7308	52	4.25701	24.9423	52	2.85199
Student	35.6250	56	6.13652	25.9464	56	3.86791	23.8393	56	3.55107
Total	34.5185	108	6.58302	25.8426	108	4.04221	24.3704	108	3.26577

In Table 6. Based on their position, students have a relatively higher average Confidentiality score than employees. Subjects from the digital native generation are not only fluent in the use of technology, but also quite understand the confidentiality aspect.

The average Integrity score did not differ based on employment status, the average difference was very small between the two groups, and in general also indicated a lack of understanding of the importance of integrity in information, both when sending and receiving. This means that they never critically consider the risk of data or information that may be distorted or disinformation.

Employees have a relatively slightly higher average availability compared to students; it can be interpreted that employees are more concerned about their responsibilities and dependence on service availability or access to information. However, this A score is considerably lower than C's awareness of secrecy.

Qualitative Data-based map:

This participatory observatory involved local volunteers from various digital literacy programs conducted by Tular Nalar and Siberkreasi. The educational maps gathered are as followed:

Tular Nalar employed an interactive method to educate the audience on digital literacy supported by the experts of media and digital literacy. The aim is to improve society's awareness, response, and consciousness in critical thinking facing the misinformation floods. To handle deficiencies in critical thinking, Tular Nalar constructed 8 competencies, divided into 3 levels, and elaborated into 8 themes, as shown in Tabel 7.

Table 7: Tular Nalar Curriculum

Aspects	8 themes	8 Competencies
Know	Literacy Media and Digital	1. Access 2. Managing Information 3. Message construction 4. Processing Information 5. Message Sharing 6. Building Self-resilience 7. Protecting Data 8. Collaboration
	Pre-service students	
Act	Active Citizenship	
	Misinfodemic	
	Digital parenting	
Tough	Intolerant and discrimination	
	Mitigation and Disaster	
	Disability	

Source: tularnalar.id

Tular Nalar offers two learning options: Online learning and Training-to-Trainer (TTT). Online learning aims to exercise critical thinking with practical digital literacy. This option is open to anyone from many backgrounds. While the TTT option aims to deliver a full curriculum of digital literacy at each level. The online learning or TTT course are equipped with videos and quizzes, so the learning becomes entertaining, fun, and enlightening. This education is general, meaning not targeted at a specific audience. This digital literacy movement is supported by 40 facilitators, who had special preparation training. Currently, this movement has successfully delivered 1200 webinars. After the Covid-19 pandemic, it is expected to have offline/onsite events with more specific audiences, such as youth or the elderly. Meanwhile, participatory observation at Siberkreasi showed the overlapping content of digital literacy contents. Siberkreasi is the massive digital literacy movement led by the Ministry of Communication and Information of the Republic of Indonesia. Siberkreasi is a national effort in fighting the greatest potential danger faced by Indonesia, namely the fast and wide spreading of negative content through the internet, such as hoaxes, cyberbullying, and online radicalism. Government's countermeasures against those negative contents by socializing digital literacy in many sectors, especially education. For example, by adopting digital literacy materials to the formal curriculums. This movement also encourages people to actively participate in producing positive content on the internet and become more productive in digital media. Siberkreasi's vision is to educate Indonesian society in digital literacy. Its mission is to enhance digital literacy in Indonesia, massively and sustainably promoting positive content, and pushing the

URL: http://doi.org/10.14738/abr.1307.19110

millennial generation to productively create positive content in the virtual world. The activities are not specifically targeted, meaning heterogenous. Most of the activities are online with clustered audiences per region, by collaborating with various speakers and local governments. Nationality is emphasized in all of the material developed by Siberkreasi. So far, Siberkreasi has reported more than 2500 webinars with 9500 literate and 6000 partners. Learning materials of Siberkreasi consist of four pillars: digital skills, digital culture, digital ethics, and digital safety. The details of the four pillars are presented in Table 8.

Table 8: Siberkreasi Learning Contents

Pillar	Contents
Digital Skills	Digital Literacy and Digital Skills
	Reviewing Digital Landscape
	Navigating Information Search Engine
	Understanding Conversational and Media Social App
	Getting familiar with Digital Wallet, E-commerce, and Digital Transaction
Digital Culture	Digital Culture in Strengthening National Character of Modern Citizen
	Internalization of National Principles: Pancasila and Bhineka Tunggal Ika, as Digital Citizen
	Cultural Digitalization and ICT
	Love Domestic Products
	Digital Rights
	Digital Communication Culture in Indonesia Society
Digital Ethics	Introduction to Digital Media Ethics
	Let's Talk about Digital Society Netiquette Challenges
	Beware of Negative Contents
	Meaningful Interaction in Digital Space
	Let's Interact and Transact wisely
	Digital Media does not change Human beings
Digital safety	Secure Yourself and Friends in the Digital Space
	Protecting Digital Devices
	Securing Digital Identity and Private Data in Digital Platforms
	Understand and Avoid the Digital Scams
	Securing Digital Footprints
	Children's Security in Digital Platforms
	Digital Security Challenges

Source: siberkrasi.id

Analyzing the contents of Siberkreasi educational contents, it is evident that information security literacy has clearly been included in the modules, and delivered in various socialization activities as well as educational events. Nonetheless, the activities are in bulks and have not measured the behavior changes. Pre-test and Post-test are conducted before and after the webinars, however, the data have not been published, on whether there are any cognitive, affective, or behavioral changes. Considering the audience, the number of participants and the backgrounds are various. Participants are attracted to join the event because of the gimmick provided (e-money vouchers).

These quantitative and qualitative analyses then became the rationale of the educational model about digital security critical thinking to prevent and handle the VUCA situations, caused by the Information and Communication technology.

Education of Users on Security-Critical Thinking in Order to Prevent and Cope with VUCA Caused by ICT

The results of quantitative research on the digital literacy map of data security, and results from the qualitative research on the Digital Literacy Movements in Indonesia, are clearly seen a wide gap in the contents specialization and educational methods. The materials prepared and used by the two Digital Literacy movements are very general and the educational method is massive (bulk) and less personalized. Both movements emphasize more on the quantity of the number of events, the number of participants, and also the number of partners involved. There is no clear explanation about the impact on the participants' behavior change. Therefore, the impacts can only be assumed to raise awareness. This can be justified by the digital literacy index of the society which is currently still low. Digital Literacy Index of Indonesia 2021 which was published by the Ministry of Communication and Information, scored 3.9 out of 5.0 for digital culture, digital ethics with a score of 3,53, and digital skill with a score of 3.44. Meanwhile, digital safety scored lowest with 3.10 or a little bit above average. This means the majority of Indonesian people have much less information security literacy, although increasingly small in recent years.

The materials on data security from both movements are actually integrated into the digital safety module. However, since the method is a webinar with lots of other materials, and not given in-depth thru practical exercises, and no further mentoring after training, therefore behavior changes are not fully achieved.

Attention to the urgency of information security and education varies in many countries with differing contexts. In Japan, Takemura and Umino (2009) saw that continuous education is a must, and stated that seminar is one of the effective methods of building society's awareness. This finding supports that the activities of Tular Nalar and Siberkreasi movements in building awareness among the Indonesian people. It also emphasizes that extended and strengthened education should be aimed to the affection and behavioral level.

Creativity and comprehensive methods are needed for behavioral change. In this matter, Abawajy (2014) proposes several training methods and tools such as video, games, and discussion. While Kegel (2015) claims a project called PISA, Personal Information Security Assistant, which improves the privacy and security awareness of end-users by aligning the user's personal IT environment to the user's security requirements by elicitation of a user's privacy and security requirements (risk appetite), and user's risk perception. Furthermore, Olesigun and Ithnin (2013) created and implemented an information security awareness training (ISAT) program for University. This elaboration shows that training for information security literacy needs a consideration not only in content but also in method and tools. information security should become an organizational culture and information security culture embedded in human behavior (Schlienger and S Teufel, 2004; Da Veiga, 2014; Da Viega and Martins, 2020; Solomon and Brown, 2020). Interestingly Fujs, Vrhovec, and Vavpotic (2021) create a user segmentation based on human aspects of information security. This specialization

URL: http://doi.org/10.14738/abr.1307.19110

of training approach is to cope with the traditional model of training which may be unsuitable for specific audiences.

Based on the research result and the references to previous research, the gap between the material and educational methods can be overcome by a more specific model for behavior change, by more focus on the specific content of information security, methods, and tools. Therefore, we propose a model of education on security-critical thinking. This model consists of three main themes, which are live learning pathways, 21st-century curricula, and relevant specialized education. The aims are to navigate through VUCA contexts, taking into account the necessity to introduce short- and long-term responses that prepare individuals, organizations, and stakeholders for an uncertain future.

Live learning pathways will start when students enter the university. Starting from the beginning it is recommended that the university prepare them with a special event on the introduction to critical thinking toward information security. While awareness is developed, the next step is a comprehensive workshop for a small group of students. The workshop's design is based on the cohort of participants who are gen Z. Understanding the gen z characteristic will lead the design to not only consider the content but also the method to deliver, creative tools, as well as who will deliver it. The implementation of pre-test and post-test which consists of C-I-A will be embedded in the workshop program in order to evaluate the impact of the workshop. The participants in the first batch will become the agent of change.

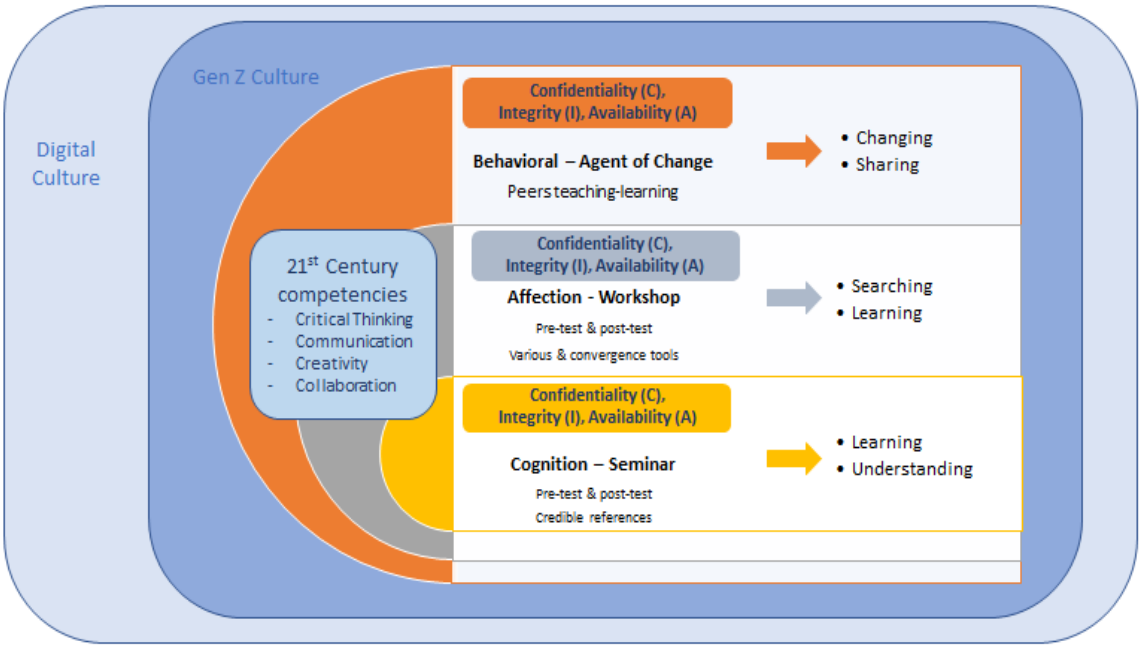

Figure 1: ISCT-CIA Education Model

They will contribute as a facilitator for the next batch and on. Therefore, the live learning pathways are constructed, and hopefully, sustain in an individual's future and influence others. The 21st-century curriculum is a curriculum that emphasizes team-based projects in which groups draw on each individual's strengths to solve problems. This model exposes students to new ideas and opposing viewpoints while demonstrating the power of the collective mind. In

the landscape of 21st-century curriculum, we understand the three skills that should develop, which are life and career skills, learning and innovation skills, and information, media, and technological skills. The education model proposed will emphasize learning and innovation skills; and information, media, and technological skills. It will implement in the context of information security literacy, which consists of the element of information security, C-I-A. Furthermore, in learning and innovation skills there are 4Cs that have to develop: critical thinking, communication, collaboration, and creativity. Therefore, implementing this concept to the model proposed is precisely suitable, with C-I-A as the specialized content education.

The described model of critical thinking on information security will be proposed as **Information Security Critical Thinking** education model or ISCT-CIA as depicted below.

CONCLUSION

To be aware of information security, especially while using digital communication, requires awareness, in thinking critically about the risk of exposing (private) information. In the survey at the Catholic University of Atma Jaya, most of the subjects are quite familiar with technology and digital devices, however, only a few understand the risks of information security aspects: Confidentiality, Integrity, and Availability (CIA). This research found that age and level of education do not correlate with the respondent's understanding of information security.

Based on the participatory observation, this research found that there are efforts from organizations and the government to increase digital literacy. Education is considered massif and lacks deeper interaction for behavioral change. Therefore, a more engaging model is needed to reach the goals of critical thinking of information security. With the convergence model which extends the massif model with the digital platform, this research proposes a combination of face-to-face communication and interaction, with mediated communication. This is a step of changing process, starting with awareness, continuing to desire to change, and behavioral change. Moreover, the person will become an agent of change for life learning, promoting the critical thinking of information security. To extend the findings, we recommend that further research should be conducted on a wider audience in Indonesia. Especially to the populations in the various provinces or islands, who have just enjoyed internet access and are prone to information security risks. Therefore, the detailed mapping could become the general situation in Indonesia and would help in developing more effective and efficient strategies to ensure information security literacy for a wider audience of Indonesian citizens.

References

Aldawood, H, Skinner, G. 2018. 'Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review', IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, pp. 62-68, doi: 10.1109/TALE.2018.8615162.

_____ (2021) https://www.internetworldstats.com/asia.htm#id

Confessore, Nicholas (2018), 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

C.N.N. Indonesia. (2020, June 26). 'Deretan Peristiwa Kebocoran Data Warga RI Sejak Awal 2020'

https://www.cnnindonesia.com/teknologi/20200623160834-185-516532/deretan-peristiwa-kebocoran-data-warga-ri-sejak-awal-2020

URL: http://doi.org/10.14738/abr.1307.19110

De R, Pandey N, Pal A. 2020. 'Impact of digital surge during Covid-19 pandemic: a viewpoint on research and practice'. International Journal of Information Management 55(1):102171. DOI 10.1016/j.ijinfomgt.2020.102171.

Da Veiga, Adéle (2016) 'Comparing the information security culture of employees who had read the information security policy and those who had not' ; Illustrated through an empirical study, Information & Computer Security ; volume 24, issue 2, page 139-151 ; ISSN 2056-4961, https://dx.doi.org/10.1108/ics-12-2015-0048

Da Veiga, Adele; Martins, Nico (2020) Improving the information security culture through monitoring and implementation actions illustrated though a case study, http://hdl.handle.net/10500/26784

Fujs, D., Vrhovec, S., Vavpotic, D. (2021) Know Your Enemy: User Segmentation Based on Human Aspects of Information Security, IEEE Access, Vol 9, Pp 157306-157315 (2021), https://doi.org/10.1109/ACCESS.2021.3130013

Ibrar Bhatt & Alison MacKenzie (2019) 'Just Google it! Digital literacy and the epistemology of ignorance', Teaching in Higher Education, 24:3, 302-317, DOI: 10.1080/13562517.2018.1547276

Jemal Abawajy (2014) 'User preference of cyber security awareness delivery methods', Behaviour & Information Technology, 33:3, 237-248, DOI: 10.1080/0144929X.2012.708787

Katadata (2021), 'Penetrasi Internet Indonesia urutan ke-15 di Asia pada 2021' https://databoks.katadata.co.id/datapublish/2021/07/12/penetrasi-internet-indonesia-urutan-ke-15-di-asia-pada-2021 Accessed 20 March 2022

Kegel, Roeland H.P. Kegel (2015) 'The Personal Information Security Assistant', http://purl.utwente.nl/publications/100508

Liu, Liyuan & Han, Meng & Wang, Yan & Zhou, Yiyun. (2018). 'Understanding Data Breach: A Visualization Aspect'. 883-892. 10.1007/978-3-319-94268-1_81.

Marcus Leaning (2017). 'Media and information literacy: an integrated approach for the 21st century'. Chandos information professional series

Naumovski, T, Taneski, N. 2019. 'Social engineering in the context of cyber security', 10th International scientific conference the great power influence on the security of small states, 1. pp. 282-292. ISSN 987-608-4828-46-4 (2019-06-23). http://eprints.ugd.edu.mk/22241/

Phillips, Fred. (2012). 'Social Capital, Social Engineering, and Technopolis'. World Technopolis Review. 1. 86-91. 10.7165/wtr2012.1.2.86.

Reinard, John C. (2006) 'Communication Research Statistics', Sage Publication, London, New Delhi

Statista (2021), 'Statistics and Facts About Social Media Usage, on the internet' www.statista.com/topics/1164/social-networks. Accessed 17 March 2022

Siberkreasi: Makin Cakap Digital http://siberkreasi.id

https://www.kominfo.go.id/content/detail/39488/siaran-pers-no-15hmkominfo012022-tentang-budaya-digital-membaik-indeks-literasi-digital-indonesia-meningkat/0/siaran_pers

https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

Olusegun, Oyelami Julius and Ithnin, Norafida (2013) 'People are the answer to security: establishing a sustainable Information Security Awareness Training (ISAT) program in organization', http://eprints.utm.my/40980/,

Samonas, S., & Coss, D.L. (2014). 'The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security'.

Schlienger, T; Teufel, S. (2004) 'Information security culture - from analysis to change: research article', South African Computer Journal; Vol 31 (2003), http://ajol.info/index.php/sacj/article/view/18594

Grant Solomon, Irwin Brown (2020) The influence of organisational culture and information security culture on employee compliance behaviour, Journal of Enterprise Information Management; volume 34, issue 4, page 1203-1228; ISSN 1741-0398, DOI: https://dx.doi.org/10.1108/jeim-08-2019-0217

World Economic Forum. '2021. Skills for the 21st Century' https://www.weforum.org/projects/skills-for-the-21st-century

Takemura,T. and Umino A. (2009) 'A Quantitative Study on Japanese Internet User's Awareness to Information Security: Necessity and Importance of Education and Policy', https://zenodo.org/record/1078104

Terry Anderson and Julie Shattuck. (2012). 'Design-Based Research: A Decade of Progress in Education Research?' Educational Researcher 2012 41: 16, DOI: 10.3102/0013189X11428813

https://www.kominfo.go.id/content/detail/39488/siaran-pers-no-15hmkominfo012022-tentang-budaya-digital-membaik-indeks-literasi-digital-indonesia-meningkat/0/siaran_pers

TularNalar Untuk Pengajar – TularNalar https://tularnalar.id/untuk-pengajar/