Employees' Impact on Cyber Security

Human Behavior Consequences on security measures

Dr. Magda Lilia Chelly
Managing Director | Responsible Cyber Pte. Ltd.
25A, Smith Street, Singapore, Singapore
mchelly@responsible-cyber.com

Abstract—**The increase of connected devices and various technologies has resulted in changes in human behavior – People are relying more on online communications instead of face to face or telephone conversations.**

The article describes the importance of focusing on human factors in a cyber-security strategy. It reviews the existing approaches, including methods analyzing root behaviors. Several metrics are tailored, and practical cases are described, including gender impact.

The article lists several pieces of studies showing that often, employees do not comply with guidelines and policies, and many may not even that these exist. It studies the methodology to decrypt people's attitude and knowledge.

The objective is to identify fundamentals that would help further investigation and improve the development of cyber security strategies based on current literature and research. The results outlined in this article present a need for the cyber security field to adopt a proactive approach towards human behavior.

Keywords-component; Information security Gender impact Human Behaviour Awareness Risk Culture

I. Introduction

Human behavior is one of the most complex sciences. It covers different areas including behavior towards new technologies and cyberspace.

A lack of consideration and adaptability for cultural differences and behavior is often found among organizations' strategies, in general, and among cyber-security approaches, in particular. Leaders expect employees to adopt new cyber-security policies, procedures, practices overnight, denying the validity of external factors like cultural, language or gender impacts.

The Chief Information Security Officer's expectation is that all employees should be compliant, and responsive to authority, guidelines, and policies. The employee is expected to conform to the company's standards, independent of geographical and cultural differences.

Companies who adopt this attitude with regards to their cyber-security strategy are at risk. A robust cyber-security strategy needs to be sensitive to cultural differences which would influence employees' behavior and productivity.

This article highlights the importance of integrating human factors, culture influence, and gender into a cyber-security strategy. In the analysis, we define different technology applications across various countries and continents. The usage varies and is different for individuals with diverse backgrounds.

In the second part of the paper, we investigate employee response to a cyber-security survey. We analyze cyber-security awareness program metrics, and evaluate two approaches: a traditional approach and a second approach that takes into consideration industry, culture, gender and language backgrounds. Examples of cyber-strategies and methods are also listed and compared.

We studied:

- Technological, behavioral patterns and analysis between Asia, Middle East and Europe
- Comparison and effectiveness analysis of Cyber Security Awareness Programs in these countries
- An experimental case study conducted within a group of financial professionals in Asia

The aim of this paper is to highlight the importance of aligning external human factors in the cyber-security strategy.

II. CYBER SECURITY MATURITY: BETWEEN TECHNOLOGY AND HUMANS

This section describes general trends in technological usages in different cultures.

As cultural backgrounds define how people behave and interact, cyber security strategies need to take into account the cultural characteristics of the organization.

The following shows a comparison of internet penetration in Asia, Europe, and The Middle East/North Africa (MENA.) Numbers and figures have been extracted from a survey made by ICTQatar.

A. *Internet*

Whilst the internet is now a common well-recognized network and technology, Table 1 illustrates that just less than half the world's population is currently connected.

TABLE I. INTERNET PENETRATION

World Internet Usage		
World Region	***Internet Users (June 2016)***	***Penetration (%)***
Asia	1,801,512,654	44.50%
Europe	614,979,903	73.90%
Middle East	141,489,765	57.40%
World Total	3,631,124,813	49.50%

Source: internetworldstats.com

Table 1 shows differences between the three continents. Europe – with the smallest population base among the three regions – shows the highest percentage of population using the internet whilst Asia – with the largest population base and less than 50% internet penetration – at the bottom of the list with approximately 30% less Internet penetration than Europe.

MENA shows better connectivity than Asia with 57% of the population using the internet.

It is evident that despite the technological tsunami in recent years, many individuals are still without access to the Internet whilst it has become the most important tool for businesses, from start-ups to multinational corporations and governments. This fact raises two important questions:

- How can an organization reach out to a population without Internet?
- How can an organization collaborate with a population not used to the Internet?

We will explore these issues from the perspective of Start-ups, Multinationals, and Governments.

- Both governments and multinationals in Asia and the MENA communicate mainly through paper-based documents.
- Start-ups and multinationals collaborate in these regions with their employees mainly through phone communications, face to face meetings and paper-based documents.

These examples clearly define processes that are different from the newest communication avenues in Europe. Intra-organization communication has to adapt to the country's technological limitation and the employees' routines.

B. *Emails*

Electronic mail has become the standard way of swapping digital messages between computer users. Nowadays, email has been recognized as a legitimate and formal form of communication by business, governments and non-governmental organizations across the World. Nonetheless, its usage differs from one country to another and from one continent to another.

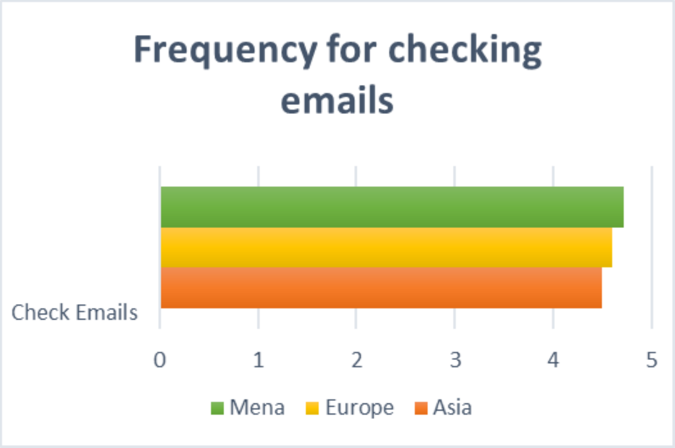


Figure 1. Email usage, 1 = Never 2 = Less than monthly 3 = Monthly 4 = Weekly 5 = Daily, Source: ICT Qatar, July 2014

Figure 1 illustrates the email usage frequencies for different regions. Europe and the MENA Internet users check emails almost daily. Asia Internet users check their emails the least frequently. There is a clear correlation between Internet penetration and email usage frequency.

A separate study comparing internet user activity in four countries – France, Qatar, Tunisia and Indonesia – between 2013 and 2016 suggests major differences between MENA and Asia Internet users' activities and Europe. This study was conducted on the banking, construction, and consumer goods industries.

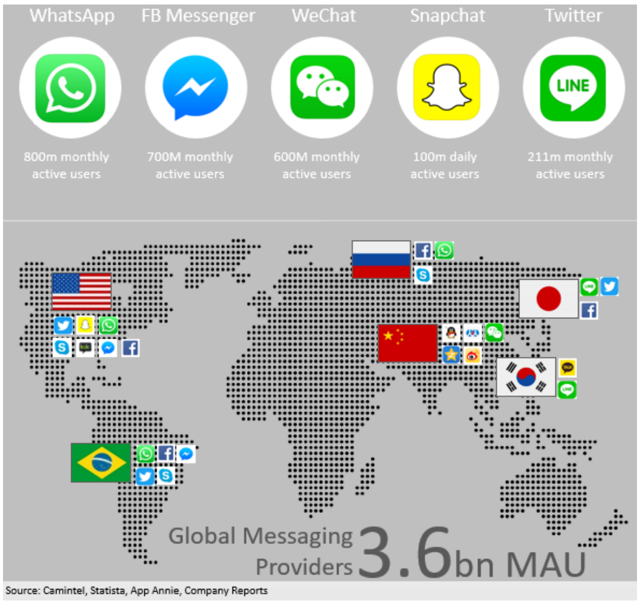
Emails have been significantly used for business in Europe with high response rate – 80% replies within 72 hours. In MENA and Asia, business emails have been reported to be unanswered for months. MENA business Internet users are significantly less likely to interact with third parties over emails, preferring to make Internet calls instead.

C. *Instant Messaging*

Instant messaging is a very popular way to share communication instantly with friends, colleagues and family members.

The most frequently used instant messaging platforms include Facebook, WhatsApp, WeChat, LINE, and Viber. Facebook is most popular platform globally, with WeChat and WhatsApp expanding exponentially.

Instant Messaging has become a part of daily life and therefore an integral part of any business. Where instant messaging is used in their personal lives, internet users would also approach third parties for business purposes through this avenue. Today, Instant Messaging is routinely used in product and service advertisements, internal and external corporate communications, and business to business dealings. Instant Messaging is slowly replacing e-mail as the baseline tool for online communications.


WhatsApp
FB Messenger
WeChat
Snapchat
Twitter
LINE
800m monthly active users
700M monthly active users
600M monthly active users
100m daily active users
211m monthly active users
Global Messaging Providers
3.6bn MAU

Source: Camintel, Statista, App Annie, Company Reports

Figure 2. Global Instant Messaging Leaders by Country, Source: Camintel, Statista, August 2015

Figure 2 shows the instant messaging leaders by country. The most popular Instant Messaging platforms vary from one country to another and therefore from one continent to another, reflecting linguistic, economic, and sociopolitical or cultural differences. Facebook is dominant in English-speaking space. WeChat, a Chinese platform dominates Asian markets. LINE is popular in Japan while KakaoTalk is leading in South Korea.

MENA region users are more likely to utilize Facebook, WhatsApp, and Viber, indicating usage by English speakers.

D. *Communication Channels and Cyber Strategy*

This increased use of and dependence on new cyberspace technologies has brought in new risks. Businesses are increasingly aware of how critical human factors are in the overall cybersecurity strategy and have started implementing cyber-awareness programs. These programs are usually based on e-learning or phishing simulations.

Of the range of solutions that are currently available in the market, the predominant ones provide standard services to companies with standard presentations or predefined templates for phishing simulations. The previous analysis has shown the differences in technology usage by continents. This has to be a key element to consider for an effective cybersecurity approach for business.

A case study was conducted with a global consumer goods company, selling online women attire. The company has main offices in France, Indonesia, and Qatar. Qatar and Indonesia Internet users are less likely to make online acquisitions compared to France. This fact led the company to implement different operational processes for the three countries. Employees in France communicate internally through official communication channels and have back up all in writing on company email. Employees in Tunisia communicate with their colleagues and customers through Facebook messaging or phone calls and keep little transactions records. Employees in Qatar use WhatsApp and phone for their purchases, also with very little transaction records.

The company - which did not provide for customization but had a dedicated email to receive customer requests – decided to launch a cyber-awareness program using phishing simulation through email targeting 100 employees across the three countries. The phishing email centered on a customized order request for a woman's dress and had an attachment with a .jpg extension.

21% of the users opened the phishing email. This number is considered a metric for various awareness campaigns and phishing simulations. The key point in this example is that an email-based phishing simulation and the metrics resulting from the experiment is not effective. The employees did not use emails for their business communications with their colleagues and customers in Tunisia and Qatar and by default, the phishing email was not opened.

This case study shows that the exposed risk surface changes from one country to another. The employees are not using the same channel of communication and therefore they are subject to different cyber risks.

Following this practical case study, we suggest an improved program taking into consideration different cultures and internet usages. Table 2 provides a view of the proposed assessment.

TABLE II. ASSESSMENT MATRIX

Usage for Business			
World Region	***Email***	***WhatsApp***	***Facebook***
Asia: Indonesia	Medium	High	Medium
Europe: France	High	Low	Low
Middle East: Qatar	Low	High	High

Often, security professionals do not adapt their global cybersecurity strategies/awareness programs to different linguistic, economic, and sociopolitical differences. They need to take into consideration culturally determined behavior to achieve effectiveness. It is imperative that security professionals practice flexibility and adaptability for culturally different behavior and country based common usages. A cybersecurity strategy is best judged by how well it is suited for the targeted environment.

To better serve their responsibilities and mitigate the cyber risks, security professionals need to develop an awareness of how cultural background affects usage, behavior, and attitude. Via behavioral and cultural management procedures, security professionals can create an effective cyber-awareness program that addresses all the employees, globally. The most important step to achieve this, is to critically examine differences in cultural behavior and Internet usage across the business geographical presence, before rolling the program.

E. Risk Profiles and Cyber Strategy

The cybersecurity strategy or cyber-awareness program goal is to reduce the human factor risk. The strategy or program sets out actions to take to reduce the risk and secure business and individuals [1].

According to the analysis in "Human Behaviour as an aspect of Cyber Security Assurance" [2] the most popular form of cyber risk assurance is cybersecurity risk assessment. 64% of organizations are adopting this method. To be effective, the organizations need to understand the requirements and communicate the results. However, methods of cybersecurity assurance have not been evolved to match the target environment.

The most striking element, however, lies in the key differences. The extend of these differences may considerably impact the risk assessment. The survey in Figure 3 shows the diverse perception of risks by an individual from different cultures and continents.

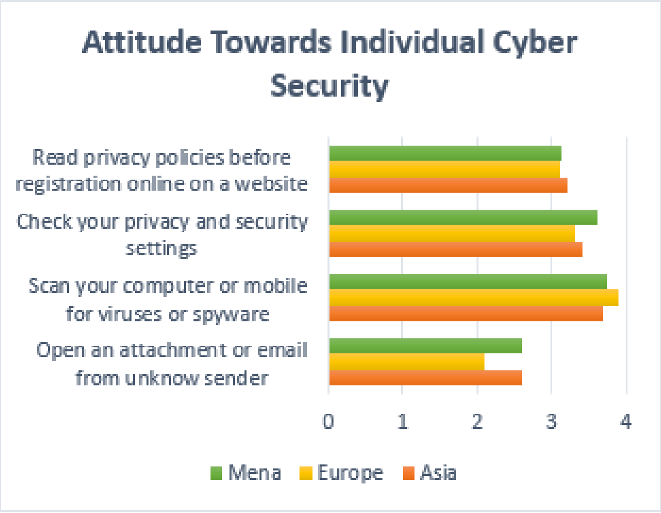


Figure 3. Attitude Toward Cyber Security, Never 2 = Seldom 3 = Sometimes 4 = Often 5 = Always, Source: ICT Qatar, July 2014

Figure 3 indicates the different maturity levels of the users. Europeans Internet users are less likely to open an email from an unknown user while Asian and MENA users are much more likely to do so. European Internet users are also more vigilant about scanning their devices for viruses or malware comparing to Asian or MENA users. On the other side, MENA users are more careful around privacy settings online. These different attitudes are related to cultural and sociopolitical characteristics.

Users from different cultures do not have the same level of cyber maturity. They do not recognize the cyber risk or do not perceive it in the same way. An unaware user of the danger or the consequences of his actions denotes a high risk for the organization. This study encourages incorporating individuals' cultural, linguistic and sociopolitical aspects to create a cyber risk assessment with a human factor framework. Other researches in the same field have been conducted. They identify the significant metrics related to culture, and assimilate them within the Human Factors Framework [3].

III. CYBER SECURITY AWARENESS PROGRAMS

This section includes a comparison of existing cyber-security strategies and awareness programs. The main popular solutions for cybersecurity awareness are as per below:

- Awareness instructor-led courses: A cybersecurity professional will deliver awareness courses to the employees face to face. Courses are usually for targeted small group. They address general topics like password security or email security.
- Awareness e-learning Courses: Online courses are courses around cybersecurity most common topics like emails security, password security. These courses are mainly followed by an online assessment.
- Awareness campaigns: The awareness campaigns include events, posters, newsletters, etc. They can also be rolled out as events: awareness week or awareness month.
- Awareness content: Some professionals opt for a cybersecurity blog or feed on their internal portal. This content is updated on a regular basis and allows employees to read about the latest threats and practices.
- Awareness phishing simulations: Phishing simulation solutions are based on template emails. They describe various scenarios and send them to the employees. The employees' response measures the employees' awareness. The metrics are very similar to a marketing campaign metrics: the number of open emails, the number of clicks, etc.

A cybersecurity awareness program is a change program. The most effective programs are the ones combining different solutions over a certain time. A critical point for success remains management and board's support to achieve the results. It leads to the involvement of all the organizational levels and the different departments.

Every awareness-program needs to define initial metrics to be collected and measured throughout the rollout. This is crucial to demonstrate the effectiveness of the program. The standard metrics include attitude surveys or phishing simulation metrics. Additional metrics like the number of incidents are also part of the baseline.

The duration of the awareness programs is usually one year with monthly specific topics, with language customizations. However, sociopolitical aspects or cultural differences are not part of the assessments or programs [4]. In the research undertaken by Shari Lawrence Pfleegera and Deanna D. Caputob in 2012, [5] the behavioral science improves significantly the results of a cyber-awareness program. It increases the effectiveness through incorporating the findings into the program design, development and rollout.

IV. CASE STUDY

This section of the article is providing a description of risk profiles. The risk profiles are enumerated and compared.

The below case study illustrates a maturity level assessment for individuals in the financial sector. We conducted a survey on eleven individuals working in the financial sector with no previous knowledge in the cybersecurity field. This assessment was based on a survey with technical questions and behavioral attitude questions.

We have rolled out the questionnaire on mix gender people within an average age of 38 years. The oldest individual was 58 years old, and the youngest was 22 years old.

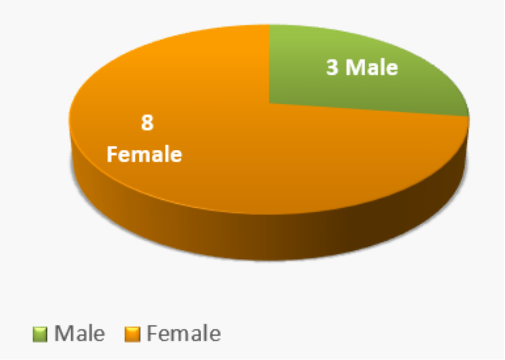


Figure 4. Gender Consitution

Figure 4 shows the number of individuals questioned. Female individuals were predominant in the study. All the participants were questioned about cybersecurity meaning. Figure 5 illustrates the results.

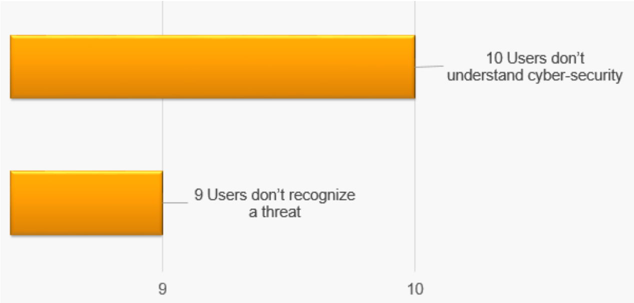


Figure 5. Assessment results

Figure 5 identifies two critical points. Individuals did not understand cybersecurity meaning. The interviewed professionals assimilated cybersecurity only to hardware or software solutions. More than half of the individuals did not think they have been through a suspicious activity before the questionnaire. They did not recognize online threats like scams, phishing or other similar activities.

Individuals, despite very important government compliance obligations in the sector and guidelines around cybersecurity and data privacy, did not have the knowledge of their risks while online. Without exception, they all agreed that they are concerned about their safety online. However, four users did not change their passwords on a regular basis.

This simple case study is showing the importance to address the environment, industry and acknowledge differences. In fact, the group of individuals had different Internet usages. They have been also submitted to their employer's policies and had a good view of the compliance requirements and regulations.

As per a research in 2015, [5] we could confirm that older users were less knowledgeable about Internet security. Having a better understanding of online security could impact positively the effectiveness of a cyber-awareness program.

This practical example encourages us to define risk profiles based on human behavior, cultural behavior, industry knowledge and behavioral patterns. We outline three risk profiles in this paragraph:

- High-risk Profile: It describes individuals not recognizing online risks and having very limited cybersecurity knowledge.
- Medium Risk Profile: It describes individuals with a partial cybersecurity knowledge. Individuals with compliance and guidelines knowledge.
- Low-Risk Profile: A low-risk profile is a fully cybersecurity knowledgeable individual with a wide sense of online responsibilities.

V. Conclusion

Human factors are important to take into consideration including cultural, gender, and attitude differences. In this paper, we discussed the different communication channels, their impact on human interactions online and we presented existing cyber-awareness solutions.

Then, we shared a case study for a small group of individuals not related to an IT environment. The case study and the recommendations aim to overcome cultural, sociopolitical, linguistic and gender limitations for cybersecurity awareness programs effectiveness.

Our proposal is based on an extended initial assessment focused on human behavior and cybersecurity understanding.

Both human patterns and cybersecurity knowledge have an important impact on the awareness results. This impact contributes in enhancing the reliability of the program and the overall cyber strategy.

A customized cyber-awareness strategy allows to build better campaigns and implement effective cybersecurity measures. In leads to an optimized business protection.

References

[1] Yogesh Malhotra, “Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation," September 15, 2015.

[2] Mark Evans, Leandros A. Maglaras*, Senior Member, IEEE, Ying He and Helge Janicke, “Human Behaviour as an aspect of Cyber Security Assurance," January 2016.

[3] Diane Henshel, Char Sample, Mariana Cains, Blaine Hoffman, “Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers” , Advances in Human Factors in Cybersecurity, Volume 501 of the series Advances in Intelligent Systems and Computing pp 123-137, 10 July 2016.

[4] Wayne Patterson, Cynthia Winston, Lorraine Fleming, “Behavioral Cybersecurity: Human Factors in the Cybersecurity Curriculum”, Advances in Human Factors in Cybersecurity, Volume 501 of the series Advances in Intelligent Systems and Computing pp 253-266, 10 July 2016.

[5] Shari Lawrence Pfleegera, Deanna D. Caputob, “Leveraging behavioral science to mitigate cyber security risk”, Volume 31, Issue 4, June 2012, Pages 597–611.

[6] Whitty Monica, Doodson James, Creese Sadie, and Hodges Duncan. “Cyberpsychology, Behavior, and Social Networking: Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords”, January 2015.