Refereed Paper Proceedings

KM2022 Conference Sponsoring Schools and Organizations:

University of Maribor
Faculty of Criminal Justice and Security

Fakulteta za informacijske študije
Faculty of information studies

s&t

Lekarna Ljubljana

International Institute for Applied Knowledge Management

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

KM2022 Conference Partner Organization:

Telekom Slovenije

Table of Contents

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2022 – Ljubljana, Slovenia

A Publication of the International Institute for Applied Knowledge Management

Conference Chairs, Local Organizers, Program Committee, and Editorial Team

KM2022 Conference Co-Chairs

Boštjan Delak
Faculty of Information Studies, Slovenia
bostjan.delak@fis.unm.si

Igor Bernik
Faculty of Criminal Justice and Security, Slovenia
Igor.Bernik@fvv.uni-mb.si

KM2022 Local Conference Organizers and Coordinators

Blaž Markelj
Faculty of Criminal Justice and Security, Slovenia
blaz.markelj@fvv.uni-mb.si

Simon Vrhovec
Faculty of Criminal Justice and Security, Slovenia
simon.vrhovec@fvv.uni-mb.si

KM2022 Conference Organizers and Coordinators

Yair Levy
Nova Southeastern University, FL, USA
levyy@nova.edu

Shonda Brown
IIAKM, USA
registration@iiakm.org

Michelle M. Ramim
Nova Southeastern University, USA
michelle.ramim@gmail.com

Nathan White
Central Washington University, USA
nathan.white@cwu.edu

KM2022 Conference Workshops Co-Chairs

Christiaan Maasdorp
Stellenbosch University, South Africa
chm2@sun.ac.za

Celina Sołek-Borowska
Warsaw School of Economics, Poland
csolek@sgh.waw.pl

Online Journal of Applied Knowledge Management (OJAKM) – Editorial Board Leadership

Meir Russ –
Editor-in-Chief

University of Wisconsin - Green Bay, USA

russm@uwgb.edu

Aino Kianto –
OJAKM Senior Editor
LUT School of Business and Management, Finland
Aino.Kianto@lut.fi

Yair Levy –
OJAKM Senior Editor

Nova Southeastern University, FL, USA

levyy@nova.edu

Ewa Ziemba –
OJAKM Senior Editor

University of Economics in Katowice, Poland

ewa.ziemba@ue.katowice.pl

Carla Curado
OJAKM Associate Editor
ISEG - University of Lisbon, Portugal
ccurado@iseg.ulisboa.pt

Nitza Geri
OJAKM Associate Editor
The Open University of Israel, Israel
nitzage@openu.ac.il

Oliver Jokisch
OJAKM Associate Editor

HSF University of Meissen, Germany
oliver.jokisch@hsf.sachsen.de

Federico Niccolini –
OJAKM Associate Editor

University of Pisa, Italy
federico.niccolini@unipi.it

KM2022 Program Committee Co-Chairs

Melissa Carlton
Houston Baptist University, USA
mcarlton@hbu.edu

Jean-Henry Morin
University of Geneva, Switzerland
Jean-Henry.Morin@unige.ch

Molly Cooper
Ferris State University, USA
MollyCooper@ferris.edu

KM2022 Program Committee Members

Paul Alpar	Philipps University at Marburg, Germany
Amy Antonucci	Western Governors University, USA
Gunnar Auth	HSF University of Applied Sciences, Germany
Michael Bartolacci	Penn State University, USA
Dizza Beimel	Ruppin Academic Center, Israel
Ofir Ben Assuli	Ono Academic College, Israel
Eric Berkowitz	College of Lake County, USA

Carlene Blackwood-Brown	Seneca College, Canada
Ina Blau	The Open University of Israel, Israel
Marko Bohanec	Jožef Stefan Institute, Slovenia
Celina Solek-Borowska	Warsaw School of Economics, Poland
Michal Borowy	Warsaw University of Life Sciences, Poland
Steve Bronsburg	Nova Southeastern University, USA
Shonda Brown	Middle Georgia State University, USA
Brian Buckles	National Defense University, USA
Michael Burt	Prince George's Community College, USA
Witold Chmielarz	University of Warsaw, Poland
Dimitar Christozov	American University of Bulgaria, Bulgaria
Malgorzata Cieciora	Polish-Japanese Academy of Information Technology, Poland
Carla Curado	ISEG - University of Lisbon, Portugal
Beata Czarnacka-Chrobot	Warsaw School of Economics, Poland
Bostjan Delak	Faculty of information studies, Novo Mesto, Slovenia
Horatiu Dragomirescu	Bucharest University of Economic Studies, Romania
Helena Dudycz	Wroclaw University of Economics, Poland
Monika Eisenbardt	University of Economics in Katowice, Poland
Ruti Gafni	Tel-Aviv Yaffo Academic College, Israel
Nitza Geri	The Open University of Israel, Israel
Michal Golinski	Warsaw School of Economics, Poland
Tirthankar Ghosh	University of West Florida, USA
Michał Goliński	Warsaw School of Economics, Poland
Jose Luis Guerrero-Cusumano	Georgetown University, USA
Julita Haber	Fordham University, USA
Meliha Handzic	International Burch University, Bosnia and Herzegovina
Wilnelia Hernandez	WH-Consulting, Puerto Rico
Angel Hueca	Carnegie Mellon University, USA
Pedro Isaias	University of New South Wales (UNSW – Sydney), Australia
Dorota Jelonek	Czestochowa University of Technology, Poland
Oliver Jokisch	HSF University of Meissen, Germany
Sathish Kumar	Cleveland State University, USA
Anne Kohnke	University of Detroit Mercy, USA
Gila Kurtz	HIT - Holon Institute of Technology, Israel
Yair Levy	Nova Southeastern University, USA
Christiaan Maasdorp	Stellenbosch University, South Africa
Eliel Melon	University of Puerto Rico, Puerto Rico

Kim Muschalek	San Antonio College, USA
Federico Niccolini	University of Pisa, Italy
Sergio Nunes	ISEG - University of Lisbon, Portugal
Mírian Oliveira	Pontifical Catholic University of Rio Grande do Sul - PUCRS, Brazil
Ilona Paweloszek	Czestochowa University of Technology, Poland
Michal Pietrzak	Warsaw University of Life Sciences, Poland
Margarida Piteira	ISEG - University of Lisbon, Portugal
Mia Plachkinova	Kennesaw State University, USA
Przemyslaw Polak	Warsaw School of Economics, Poland
Tommy Pollock	Nova Southeastern University, USA
Daphne Raban	University of Haifa, Israel
Michelle Ramim	Nova Southeastern University, USA
John-David Rusk	University of North Georgia, USA
Vincent Ribiere	Bangkok University, Thailand
Meir Russ	University of Wisconsin - Green Bay, USA
Joanna Santiago	ISEG - University of Lisbon, Portugal
Dara Schniederjans	University of Rhode Island, USA
Sara Scipioni	University of Pisa, Italy
Tamar Shamir-Inbal	The Open University of Israel, Israel
Ingo Siegert	Otto von Guericke University, Germany
Vered Silber-Varod	The Open University of Israel, Israel
Celina Sołek-Borowska	Warsaw School of Economics, Poland
Anna Soltysik-Piorunkiewicz	University of Economics in Katowice, Poland
K. Subramani	West Virginia University, USA
Eduardo Teixeira	University of the West of Santa Catarina - UNOESC, Brazil
Mathupayas Thongmak	Thammasat Universit, Thailand
Bruce Watson	Stellenbosch University, South Africa
Nathan White	Central Washington University, USA
Jędrzej Wieczorkowski	Warsaw School of Economics, Poland
Amir Winer	The Open University of Israel, Israel
Ewa Ziemba	University of Economics in Katowice, Poland
Rina Zviel-Girshin	Ruppin Academic Center, Israel

We would like to thank all the Program Committee (PC) members for their outstanding scholarly reviews and dedicated feedback to the authors!

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2022 – Ljubljana, Slovenia

A Publication of the International Institute for Applied Knowledge Management

The business side of social signals and nonverbal communication

[Industry Paper]

Vered Silber-Varod, The Open University of Israel, Israel, vereds@openu.ac.il

Alessandro Vinciarelli, University of Glasgow, UK, Alessandro.Vinciarelli@glasgow.ac.uk

Baruchi Har-Lev, Substrata.me, Israel, baruchi@substrata.me

Abstract

In this industry-oriented paper, we highlight the interest Business-to-Business (B2B) companies reveal in social signals and nonverbal communication. We begin by describing the key social signals that top dealmakers or business leaders display consistently. This issue, although non-technological in nature, seems to attract B2B companies who wish to build technological scaffolds for the aid of salespersons. The core question we try to observe is if we can leverage nonverbal cues to persuade and to become more influential in business, and how systems that collect these subtle cues of human behavior help us but not invades our personal zones. We also show the connection between leadership and nonverbal communication and the contribution of such systems to other markets as well.

Keywords: Social signals, nonverbal communication, interpersonal, interaction, computer-mediated communication, B2B.

Introduction

The business world is all about being persuasive and influential. Entrepreneurs and salespersons always strive to boost their persuasion skills to expand and grow their business. One way to leverage these skills is by mimicking someone we consider influential. Another way is to consult with an expert who guides on how to improve our performance skills. Do we really need those skills in the third decade of the 21st century and after two years of worldwide pandemic? Or does the image of a businessman, this ideal dealmaker, the natural born salesperson we saw in movies like *The wolf of wall street* (2013) is an image to forget? Do real life role models that are perceived as incredible negotiators, the persons who know how to "read the room" and exactly when to sell and when to buy, and know exactly when to pitch exist nowadays?

Are there any key social signals or styles that top dealmakers or business leaders display consistently? This issue, although non-technological in nature, seems to attract B2B companies who wish to crack this riddle (Gong.io, Chorus.ai, Execvision.io, SubStrata.me) and invest significant R&D resources to build technological scaffolds for the aid of salespersons.

Social signal is an umbrella term that accounts for the nonverbal behavioral cues we display while we are communicating with others in any form (Vinciarelli et al., 2009). In face-to-face interaction, social signals include our appearance and everything we do to change it (clothes, ornaments, make up, etc.), head movements (shacking, nodding, etc.), facial expressions, vocalizations (laughter, sobbing, etc.), pauses, tone of voice, posture and gesture (spontaneous hand movements, self-touching, etc.) and use of space and environment (interpersonal distances, arrangement of furniture, etc.). In written or technology-mediated communication, social signals include email timing (i.e., how much time it takes to respond to an email corresponds to social verticality and is related to power relations) (Kalman & Rafaeli, 2011), using emojis and typographic symbols, etc.

Attention to nonverbal communication started around 2000 years ago (circa 55 BC), when Cicero, a major figure in Roman history, wrote his famous book "De Oratore", an essay on public speaking (Cicero, 2021). One of the key points of the work was that it is not plainly important what you say, but also how you say it. Roughly one century later, such a message was further reinforced by Quintilian, another major Roman author, in his "Institutio Oratoria" (Quintilian, 2018), a work dedicated to the art of speaking. However, it is not until the 19th century that nonverbal communication starts being investigated in modern scientific terms, especially with the works of Darwin (Darwin, 1872) and Duchenne (Duchenne, 1876). Since then, nonverbal behavior was one of the main subjects of Social Psychology and it is now recognized as the main channel through which people convey socially and psychologically relevant messages in interaction (Richmond et al., 2008).

Despite the contributions above, along history, at least the western one, attention to social signals, was always marginal. The focus was always on the verbal content, on what is said. This can be explained by the major role of written communication, but also to the simple observation that content (what is said) is where our attention tends to be. The limited attention to nonverbal communication was also due to the fact that it was not considered a Language, with capital L, but a natural display that we share with the rest of the animal species. The point is that nonverbal communication is something we perceive and analyze unconsciously, and it is also something that we display mostly unconsciously. From that point of view, because it is not the focus of our primary attention unless we really decide to do so, it tends to be forgotten.

In the last century, scientific attention started to focus on nonverbal communication and on the methodologies to explore it (Knapp, 1972). At the end of the 20th century, scientists have gradually abandoned the idea that human beings are entirely rational while realizing that a lot in our life is also based on emotion (Kunda, 1999). Decision making studies showed that the process does not require only rationality but also some form of affective involvement (Kahneman, 2011), which is realized by social signals and nonverbal communication during the interaction process. An example of which is perceptual decision making about the most likely emotion expressed by other individuals (Dricu & Frühholz, 2020). Purchasing decisions are often rationalized a-posteriori, but in reality, our decisions are based on emotions and what we feel or like. Attachment to a brand or a celebrity or a particular product is explained by its mere look or design, less by its functionality, content, or moral aspects.

Moreover, many of our business or purchase decisions can be tied to the nonverbal communication or the approach of the salesperson or the brand presenting it. In this respect, vocalics (prosodic) aspects like the volume, the tone and intonation and the speed of speech has been argued to be crucial for effective communication (Vinciarelli et al., 2012). The manager's performance in terms of clothes, accessories, video conferencing background, or the design of the offices are all parts of *impression management* (IM), which also includes the way we present ourselves in social networking sites (e.g., Krämer & Winter, 2008; Grebelsky-Lichtman, Adato, & Traeger, 2020). The term IM refers to self-managing one's perceptions by others. According to the theory, one can manage the impressions that (s)he will make on others by practicing her/his social signals, by increasing awareness, and by adapting effective nonverbal communication cues. The "whole package" of social signaling is challenging for management and its complexity makes it hard to define a metric and to develop a more scientific measurement approach. For example, what difference a specific change of pace of your speech would make? Or would that t-shirt that you wear affect the level of competence and charisma others attribute to you? Nonverbal communication is the physical trace, the external manifestation of what we are inside, and therefore, it acts as a cue about ourselves. A tiny shift in the way we display social signals can improve or degrade the impression we convey. Consequently, one of the core questions is how we can leverage on nonverbal cues to persuade others and become more influential in business.

The Interaction as a Core Pivot

Interaction (face-to-face or technology mediated) and conversation are the main arenas of social signals. It is thanks to these latter, for example, that one of the most common phenomena in interaction can take place, i.e., social entrainment. This means that the participants adapt to the behavior of their interlocutors along the course of an exchange and, as a consequence, they tend to show similar response pace to emails (Kalman & Rafaeli, 2011; Kalman, Ballard, & Aguilar, 2021), they tend to converge towards the same vocalic traits (Weise et al, 2020), or they tend to increase the similarity in the way nonverbal cues are displayed.

Aspects of interaction that are of particular importance in business are the influence that people seek during conversation and the role of their inner motivations with regards to the outcomes. For example, persuasion is a phenomenon that takes two persons (Vinciarelli et al., 2009, Vinciarelli et al., 2012) and it is not just about convincing generic others by using one size fits all strategies, but about being capable to persuade specific individuals in a specific context. From an interaction point of view, this is reflected in three stages:

1. To create conditions for sharing the value of your message and fundamentally – for building trust;
2. To convey the impression of competence;
3. To show that you talk in the interest of the people you have in front of you and not only for your own interest (as a dealmaker).

Words alone are not sufficient to convey all these signals, and this is where social signals come forward. A salesperson should ensure that her/his nonverbal communication will show that (s)he is a person that can be trusted, that is competent, and that is acting towards a common interest. It is through these stages that it is possible to ensure that you can be more persuasive.

Some examples of what should be the typical social, or interactional, traits of top dealmakers are as follows:

- They establish a good connection with the people they are trying to involve in their deals (e.g., they show awareness of motivations and desires of their counterparts);
- They convey the message that they are working towards shared interests for all parties involved, in the sense that "a good deal is a deal that makes everybody happy";
- They establish an empathic communication, i.e., they show that they share the concerns of their counterparts and they do not impose their own point of view, but try to find the point of view which is good for all parties;
- They make it clear that they are not in competition with their counterparts;
- They show they are pleased with a conversation, regardless its business consequences.

While it might be clear, at least in principle, what the traits above mean in face-to-face interactions, the open question is how should sellers build that level of trust through empathy and all the other aforementioned attributes when they are trying to close a deal via email, video call or other digital environments?

Harnessing Technology to Detect Social Signals

One way to gain proficiency in social signals is to train and develop awareness of nonverbal communication (Chollet et al., 2021, Chollet et al., 2018). However, while being a powerful tool to benefit from interactions, full awareness of social signals is too demanding for our cognition, our brain is not designed to monitor every blink we make. How can we then harness technology to help us improve our nonverbal communication? How can technology analyze social signals to ultimately help us refine the way we are perceived or to really understand how others communicate with us?

Technology from this point of view can be of help because it can contribute to build a *feedback loop*. Exactly as an infant is learning to use language she learns the nonverbal cues of her environment, first by imitation, then by experiencing and finally by getting feedback. Machines can reproduce such a loop by detecting a certain behavior and giving us feedback about. For example, a machine can let us know when we are talking too much, when we are talking too fast, and when we are not smiling. In this way, machines can help to avoid behaviors that are likely to have negative interactional effects.

Machines can give us indications about the way we are displaying nonverbal communication and we can decide whether we keep doing "that" or we avoid doing "that" depending on whether we consider "that" to be a mistake or not. From this point of view, they can implement in a more

explicit and evident way, in a more formal way, that type of feedback loop we constantly experience with the people with whom we are interacting.

In general, when we interact with another person, we figure out intuitively what their state of mind is because we understand whether the people around us are giving positive feedback or not. With a machine, we can get that type of feedback in a more explicit and formal way and we can adapt our behavior in the same way as we do when we interact with people around us. Thus, machines can help us to benefit more from the natural processes of imitation and adaptation underlying human-human communication.

It is for the reasons above that several companies commercialize technologies at reading our behavior and providing, e.g., competence and trustworthiness scores. In one of the most ubiquitous communications – emails, technology reads the "digital body language", i.e., the social signals of the keyboard, whether it is the use of emojis, the use of caps, and using natural language processing can also detect jokes and irony, so it is not necessarily what is written but what is between the lines in those email communication.

There are two main types of social signal systems. A tracer and a recommender. A tracer will collect data about how a person behaves in a nonverbal manner and display it later for analysis. Such systems can be used for training. For example, preparing for an important job interview, as stated before, practice makes the difference. The tracer can work offline, on non-live data or it can work on live data. The recommender, on the other hand, will analyze a person's behavior in real-time and recommend the optimal course of action that will make him/her seem more competent during an interaction. For example, a recommender might suggest a consumer, a user, to talk slower during a conversation while negotiating on buying a new house.

Major features that are already being in use are:

Overview: Mapping the current social space of the communication. This can also be called the *context*: Defined as extracting the meaning in relationship to the people we are interacting with in a certain moment.

Sequence of actions and accumulative information gain: This is a sequence of *Overviews*, which results in a dynamic analysis towards robust insights. This feature is inspired by human-human interaction. As in every interaction, we have to adjust our messages and adjust them constantly towards the other person based on the feedback that we are getting from the other side. Such feedback can be an email (or *not* responding to an email), a smile, manner of speech (shouting, for example). People constantly adjust their social behavior to achieve their goals, and therefore the technology should adapt this feature.

Concluding Insights: Technology can help us to be the right person in a particular setting. Technology can be real-time adaptive for a particular interaction and to give us a probability, for example, on how our interlocutor feels in that moment about us.

Recommendations: This feature can help the user by presenting her/him the path of adaptation towards appearing more trustworthy, for example, or more competent, or to help reduce the degree of aggressive persuasion and at the same time increase the benefits to the customer messages.

Figure 1A-D demonstrates the idea behind the technology. The system, Q for dealmakers by SubStrata, is an email communication genius for B2B sales. Trained on millions of data points, it "reads between the lines" to figure out where the prospect stands and guides the salespersons through the best next actions to take to increase her chances of winning the deal. To see an analysis of the process the user clicks on the "Analyze" button (changing to "Analysis" during the action (Figure 1A)). The result contains the elements that were introduced above. The *Overview* is introduced in three different places. The first one is the *Selling zone* that shows the exchange of actions (in this case, emails) between a salesperson and a prospect and places them on top of the Selling zone. The Selling zone represents the prospect's intention to "close the deal", and accumulates the way that the salesperson is being perceived: Above the horizontal green area – the salesperson is being perceived as being too aggressive and might shy away the prospect (might be seen as *Chutzpah*); Below the horizontal green area – the salesperson is being perceived as being too complaisant and might come across as non-competent which might cause the prospect to pass on the deal; Within the green area – the salesperson is being perceived as competent and the prospect is expected to be still interested in the deal (Figure 1B). Each new email will change the position of the deal, thus representing the *Sequence of actions and accumulative information gain*. The *Upper hand* marking (Figure 1C) shows who is being perceived as more competent in a given email, the sender or the addressee. The pragmatic sentiment of the sender in a specific email allows the salesperson to see a glance of the *Concluding Insights*. Together these three elements allow the salesperson to easily map the process.

Another part of the Q for dealmakers by SubStrata is a simulator. This is a special feature that allows the salesperson to mimic a possible outcome if he will send an email draft at the time of clicking "Simulate" with the text he entered into the draft (Figure 1D). The system will assess the chances to win a deal in such a scenario and if necessary, will recommend a more suitable action to take in a given situation given the previous *Sequence of actions and accumulative information gain*.

Leveraging nonverbal information is not a straightforward task. For example, unlike extracting a syntactic sentiment from a given sentence based on the words in the sentence, nonverbal relies on extracting the meaning behind the sentence, not necessarily through the words but also through the manner the sentence is written thus providing a more pragmatic sentiment. It is also not like using a speech recognition engine that will tell us what the speaker said, rather it will put emphasis on how it was said. Generating such technologies requires us to observe the data with a new perspective.

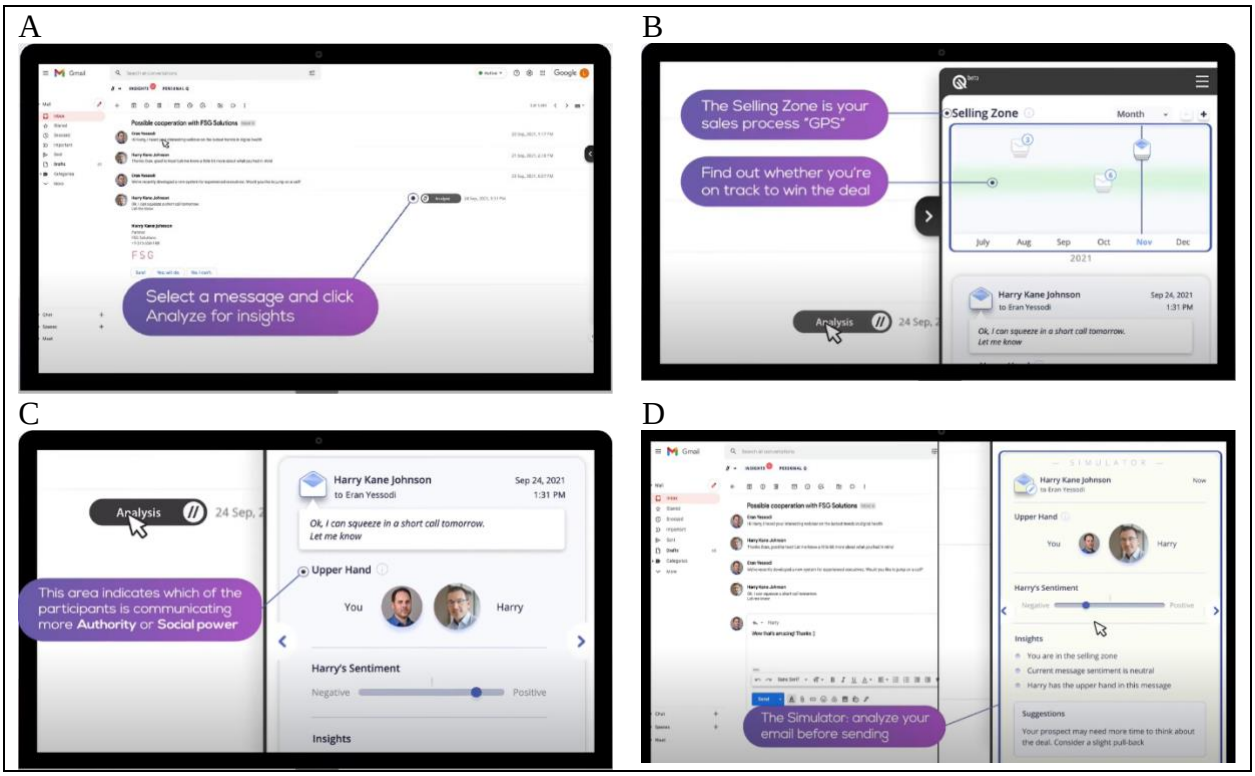


Figure 1. Four screenshots of Substrata's Q for dealmakers
https://www.producthunt.com/posts/q-by-substrata

Social Signals and Business Leadership

Nonverbal communication has a central role in the perception of business managers, their leadership, charisma, confidence, and trust. In business, leaders' nonverbal communication is essential for effective communication. Influence and persuasion are something people are sensitive to, especially during crisis situations (it could be a massive business crisis, a financial crisis or it could be a social crisis, and so on). For example, during the coronavirus years, people are oversensitive to managers' nonverbal communication (Grebelsky Lichtman, 2022) because of their stress, fear, and uncertainty. Nonverbal communication has a central effect in such periods. It affects both perceptions, cooperation behaviors, emotions, attitudes, and perceptions of their business managers. Part of it is because people have higher motivation to get updated information.

Compared to verbal information, nonverbal communication has a greater effect on listeners and when it comes to the relationship between verbal and nonverbal communication, whenever there is a discrepancy between the two, it means a break in the communication code. For example, one says that everything is fine, which implies she is calm but her nonverbal communication expresses tension. This phenomenon is called *nonverbal leakage* or verbal and nonverbal discrepancy

(Grebelsky-Lichtman, 2021) and it refers to contradicting messages in interpersonal communication. It will affect our perception not only about the message, but also about the speaker. Her trustworthiness and credibility will decrease. In every interpersonal communication, nonverbal communication has a primacy over the verbal communication. According to Grebelsky Lichtman (2022), business leaders and political leaders are highly concerned with their public image. When they consult a social signal expert, they typically want to improve their communication skills and to promote their public image. They want to influence perceptions and attitudes of others. They want to be perceived as trustworthy, credible, authoritative and yet friendly and charismatic because this may increase their influence as well as cooperation and motivation among their followers. Body language experts claim that practice makes the difference. This implies that influential nonverbal communication is not a trait a person is gifted with, but something people can acquire through training.

Contribution to Other Markets

Social signal processing could eventually be adopted for healthcare purposes. For people with autism spectrum disorder, an algorithm that signals whenever a social signal is out of context or misinterpreted can be of help. Technology can play a role in advancing their interaction skills. Other markets include support in cross-cultural communication, potentially useful in domains such as tourism and commerce in which people interact across borders. For example, tourist services providers seek for optimal performance during the discovery stage interactions. At this stage, service providers wish not to be misunderstood and that their values, as persons and as professional sellers, will be delivered without obstacles. This is where a social signal system can help. Last, Metaverse and virtual reality (VR) interactions are among the future spaces most likely to use social signals (inter alia, Aburumman et al., 2022). One potential application of this kind of research is in generating artificial agents who can teach new information and can act as a tutor who builds trust. Future research in the education market might examine the effects of nonverbal cues on students' performance, in academic video conferencing and even within VR educational settings, as Aburumman et al. (2022) suggest.

How Systems that Collect Social Signal Cues will Help Us but Not Invade Our Personal Zones?

Does Alexa know how I feel? Does it know if I am in the mood for shopping or in the mood to dim down the lights and listen to quiet music based on the speed of speech or a whispering tone? Can machines sense how we are feeling? The answer is not, not yet, but they can assess it quite well. All those signals we leave while we communicate with the devices are exploited for the analysis of our social signals. Obviously, there are privacy concerns here, though it is not different from privacy concerns that exist today with data we share with service providers. It is crucial to keep this data secured. That being said, it is important to notice that we, as humans, share many similar traits when it comes to nonverbal behavior, thus we can share less information to get such

systems more advanced. We would not want people to use social signal systems to personalize advertisements, for example. But can we prevent that? In this sense, the issue of privacy is very important for a technology that maps social signal behavior. The theoretical question is at what point collecting and processing personal information invades the privacy of individuals? Academia and research institutions already take measures to avoid leakage of personal data (Siegert et al., 2020); however, in the business market, despite some efforts that are being made (see CAHAI Ad hoc Committee on Artificial Intelligence for example (CAHAI, 2019-2021)), this is a philosophical question that still requires an answer.

Concluding Remarks

The business side of social signals and nonverbal communication was the focus of the current paper. We highlighted the interest B2B companies reveal in social signals and nonverbal communication and how technology is now ripe to systems that collect these subtle cues of human behavior. The core question we tried to tackle was if we can leverage nonverbal cues to persuade and to become more influential in business. The answer is positive but not without a privacy price. Therefore, social signal processing requires regulations to protect personal data in the business market. We showed the connection between leadership and nonverbal communication, and we showed the contribution of such systems to other markets as well.

References

Aburumman, N., Gillies, M., Ward, J. A., & Hamilton, A. F. D. C. (2022). Nonverbal communication in virtual reality: Nodding as a social signal in virtual interactions. *International Journal of Human-Computer Studies*, *164*. https://doi.org/10.1016/j.ijhcs.2022.102819

CAHAI (2019-2021). CAHAI - Ad hoc committee on artificial intelligence. https://www.coe.int/en/web/artificial-intelligence/cahai

Cicero, M. T. (2021). *De Oratore*. Arma Virumque.

Chollet, M., Marsella, S., & Scherer, S. (2021). Training public speaking with virtual social interactions: effectiveness of real-time feedback and delayed feedback. *Journal of Multimodal User Interfaces*, *16*, 17-29. https://doi.org/10.1007/s12193-021-00371-1

Chollet, M., Ghate, P., & Scherer, S. (2018). A generic platform for training social skills with adaptative virtual agents. *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS)* (pp. 1800-1802), July 10-15, 2018, Stockholm, Sweden.

Darwin, C. (1872). *The expression of emotion in man and animals*. John Murray.

Dricu, M., & Frühholz, S. (2020). A neurocognitive model of perceptual decision-making on emotional signals. *Human Brain Mapping*, *41*(6), 1532-1556. https://doi.org/10.1002/hbm.24893

Duchenne, G. B. (1876). *Mécanisme de la physionomie humaine ou analyse électro-physiologique de l'expression des passions*. Librairie J.-B. Baillière et Fils.

Grebelsky-Lichtman, T., Adato, Z., & Traeger, S. (2020). Extending impression management theory: The need for privacy vs. the need to express information on instant messaging apps. *Studies in Media and Communication*, *8*(1), 72-85. http://dx.doi.org/10.11114/smc.v8i1.4853

Grebelsky-Lichtman, T. (2021). Grebelsky-Lichtman, T. (2021). Discrepant verbal–nonverbal profile theory: Making sense of contradicting messages in interpersonal communication. In Braithwaite, D. O., & P. Schrodt (eds.) *Engaging theories in interpersonal communication: Multiple perspectives* (pp. 143-157). Routledge.

Grebelsky-Lichtman, T. (2022). On leadership & nonverbal communication. *SubStrata TV - A YouTube channel of SubStrata.me*, Jan 9, 2022. Available at: https://youtu.be/scOBCqg5CzU

Kahneman, D. (2011). *Thinking fast and slow*. Penguin.

Kalman, Y. M., Ballard, D. I., & Aguilar, A. M. (2021). Chronemic urgency in everyday digital communication. *Time & Society*, *30*(2), 153-175. https://doi.org/10.1177%2F0961463X20987721

Kalman, Y. M., & Rafaeli, S. (2011). Online pauses and silence: Chronemic expectancy violations in written computer-mediated communication. *Communication Research*, *38*(1), 54-69. https://doi.org/10.1177%2F0093650210378229

Knapp, M.L. (1972). *Nonverbal communication in human interaction*. Holt, Rinehart and Winston.

Krämer, N. C., & Winter, S. (2008). Impression management 2.0: The relationship of self-esteem, extraversion, self-efficacy, and self-presentation within social networking sites. *Journal of media psychology*, *20*(3), 106-116. https://doi.org/10.1027/1864-1105.20.3.106

Kunda, Z. (1999). *Social cognition: Making sense of people*. MIT Press.

Richmond, V. P., McCroskey, J. C., & Hickson, M. (2008). *Nonverbal behavior in interpersonal relations* (7th edition). Allyn & Bacon.

Quintilian (2018). *Institutio oratoria*. Forgotten Books.

Siegert, I., Silber-Varod, V., Carmi, N., & Kamocki, P. (2020). Personal data protection and academia: GDPR issues and multi-modal data-collections "in the wild"". *The Online*

Journal of Applied Knowledge Management, 8(1), 16-31. https://doi.org/10.36965/OJAKM.2020.8(1)16-31

Vinciarelli, A., Pantic, M., Heylen, D., Pelachaud, C., Poggi, I., D'Errico, F., Schroeder, M. (2012). Bridging the gap between social animal and unsocial machine: A survey of social signal processing. *IEEE Transactions on Affective Computing*, *3*(1), 69-87. https://doi.org/10.1109/T-AFFC.2011.27

Vinciarelli, A., Pantic, M., Bourlard, H. (2009). Social signal processing: Survey of an emerging domain. *Image and Vision Computing Journal*, *27*(12), 1743-1759. https://doi.org/10.1016/j.imavis.2008.11.007

Weise, A., Silber-Varod, V., Lerner, A., Hirschberg, J., Levitan, R. (2020). Entrainment in spoken Hebrew dialogues. In: J. Pardo, E. Pellegrino, V. Dellwo, and B. Möbius (Eds.), *Special Issue on Vocal Accommodation in Speech Communication, Journal of Phonetics, 83*. https://doi.org/10.1016/j.wocn.2020.101005

Authors Biographies

Vered Silber-Varod, Ph.D. Director of the Open Media and Information Lab (OMILab), The Open University of Israel. Former Research Fellow at the Research Center for Innovation in Learning Technologies, The Open University of Israel. Research interests and publications focus on various aspects of speech sciences, with expertise in speech prosody, acoustic phonetics, speech communication and text analytics. Honored to be part of ISCA'S WomenNSpeech list.

Alessandro Vinciarelli, Ph.D. is a full professor at University of Glasgow, where he is affiliated with both the School of Computing Science and the Institute of Neuroscience and Psychology. He is also the Director and Principal Investigator at SOCIAL AI CDT, and a member of the Advisory Board at Substrata. His main research interest is Social Signal Processing (SSP), the computing domain aimed at modelling, analysis and synthesis of nonverbal behaviour in human-human and human-machine interactions. Correspondingly, his research focuses on the inference of psychological constructs (personality, conflict, attachment, roles, etc.) from nonverbal behavioural cues automatically detected in signals captured through multiple sensors.

Baruchi Har-Lev, M.Sc., is a Co-Founder & CTO at SubStrata, a behavioral intelligence for dealmakers & sales professionals. He is a passionate tech leader with a flair for human-human & human-machine interaction, socio-affective computing and social signal processing (SSP). He has 20 years experience writing code and managing software dev teams (locally & remotely). In recent years, he has been focusing on AI/ML (DNNs, RNN/LSTM/Transformers, DQN, etc.) His special areas of expertise include Speech Processing, NLP/NLU, multimodal sentiment analysis, affect perception, interpersonal coordination & computational paralinguistics.

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2022 – Ljubljana, Slovenia

A Publication of the International Institute for Applied Knowledge Management

Cyberslacking in the academia: An examination of student's experience in an online classroom

[Research-in-Progress]

Eliel Melón, University of Puerto Rico, Puerto Rico, eliel.melon@upr.edu

Wilnelia Hernández, Independent Researcher, Puerto Rico, wiheca@hotmail.com

Abstract

The impact of the COVID-19 pandemic on the world affected several aspects of our daily life and change the way we live. Universities, schools, and all academic environments were not an exception. With those changes, students encountered different types of challenges for their academic success. Virtual environment represents a non-classroom setting that could result in a distraction for individuals during the period that they are in classes. Cyberslacking in the classroom is defined as the time that students spend doing personal activities on the Internet that are not related to class activities, like browsing social media, playing online video games, and sending messages via Short Message Service (SMS). It is possible that this kind of behavior has increased because since 2020, face-to-face students are taking classes from their homes, specifically those who were not using a virtual environment before. The visual supervising duty of the professor is limited in a virtual environment. This limitation occurred when professor has no visual contact with the students, there is no control when students access Internet during the class and the interaction between students and the professor are limited. This study will examine the cyberslacking behavior of these students and their academic success. Also, the study will compare the academic success differences between those that admit their cyberslacking behavior versus those that were not doing it. This study will use an anonymous survey as a methodology that includes cyberslacking activities and their academic success during that academic year. This study will contribute to the expansion of the cyberslacking knowledge base in academic. This knowledge should help to improve the learning process with the integration of intentional strategies that minimize cyberslacking behavior in the virtual environment.

Keywords: Cyberslacking, pandemic, behavior, virtual environment, COVID-19.

Introduction

The use of the Internet across different environment increase every day. With the COVID-19 pandemic, this increase was exponential in comparison with previous years. As a direct impact of the pandemic, schools, and universities have changed face-to-face classes to virtual ones. The attention, participation, and supervision in a virtual classroom is different than in a face-to-face setting. In a virtual environment, some students may be more easily distracted than taking in-person classes. The supervision of the professor during online classes is different from the

supervision in face-to-face classes. To increase the participation of the students and minimize the distractions, is necessary the implementation of various activities in a virtual environment. These distractions result in students engaging in non-academic activities during classes. This action should affect the learning process of the students and also should affect the grade point average. Cyberslacking is a common distraction. This concept is not a new phenomenon. In this study, we will examine the experience of the students in a virtual classroom and their engagement in cyberslacking during online classes. There are studies that confirm that cyberslacking affects the academic progress of the students, productivity a workplace environment, and other studies consider cyberslacking activities as a relief to the stress of the students or to the stress of the employees in the workplace. Furthermore, the literature is not clear about the type of cyberslacking activities that should result in a benefit for the stress. The studies agree that the amount of time for these activities can not be determined to be beneficial and non-harmful. With this study, we want to propose that universities will need to integrate orientations among their students about cyberslacking behavior as part of their first-year orientations.

Literature Review

In the next section, we present relevant literature on the concept of cyberslacking. This brief overview of literature review showed the approach of cyberslacking in an academic context. The cyberslacking section presents the definition of the term and permit the visualization of it in an academic environment. The following subsection is a theoretical view on cyberslacking to offer several studies and different perspectives on cyberslacking in the classroom. This literature facilitated understanding the harmful and the benefit of cyberslacking activities (Ravizza et al., 2014). We consider this information is valuable for the faculty members and the students. The first one is to consider the integration of new strategies to benefit the learning and academic progress of the students and increase the participation of the students during the class to minimize the temptation of engaging in cyberslacking. The second one is to teach more about cyberslacking and provide tools that help students to avoid it. There are many tools and orientations that academia provides for the first-year students to help them to have better university life. Today, is very important that academia integrate as a part of those orientations the understanding of cyberslacking and help students in the manage of it. Furthermore, to comprehend the harmful and the benefit of it and the repercussion of academic progress (Ravizza et al., 2014).

Cyberslacking

Cyberslacking is the overuse of the Internet in the workplace for purposes other than work (Whitty & Carr, 2006). In an educational context, cyberslacking is defined as the use of technology for activities for non-academic purposes (Margaretha et al., 2021). Cyberslacking in the classroom is also defined as the time that students spend doing personal activities on the Internet that are not related to the class activities, like browsing in social media, play online video games, and send messages via Short Message Service (SMS) (Gerow et al., 2010; Simanjuntak et al., 2019). Cyberslacking is considered a behavior (Simanjuntak et al., 2019). This behavior occurs when

students access the Internet during classes, and this access is not related to the material being taught. Cyberslacking affects the academic progress of the students because engaging in multi-tasking activities during classes is harmful to the attention of the students (Rosen et al., 2008; Wang et al., 2012; Junco & Cotton, 2012; Sana et al., 2013; Ravizza et al., 2014).

Theoretical view on cyberslacking

The studies about cyberslacking have different settings, but the behavior or the classification of it could apply at similar manner. Blanchard and Henle (2008) classified cyberslacking behavior as minor and serious. The classification is important to determine the harm of cyberslacking. The minor could affect only the person engaged in it, but the serious could affect others. As an example, cyberslacking could affect the bandwidth of the Internet connection, compromise personal information, and open the door for cybersecurity problems. Anandarajan et al. (2004) presented cyberslacking in two dimensions. These dimensions are: opportunities vs. threats, and organizational vs. interpersonal. Using those dimensions, Akbulut et al. (2016) showed the use of the Internet for personal purposes as disruptive, recreational, personal learning, and ambiguous use. The study by McCoy (2016) revealed that 92% of the students sent messages during class. Ravizza et al. (2014) showed the harmful result for the learning process of the students when they use the Internet for activities not related to the class. Furthermore, Wu et al. (2018) showed the negative impact that cyberslacking behavior result in the academic performance of the students. There are several factors that influence students to commit cyberslacking (Varol & Yıldırım, 2017). Studies designated demographics, motivation, self-control, self-efficacy, self-regulation, and multi-tasking as some of those factors that result in cyberslacking behavior (Varol & Yıldırım, 2017; Wu, 2017). On the other hand, Yılmaz and Yurdugul (2018) affirmed that cyberslacking behavior is related to other aspects as psycho-social perceptions, attitudes, and learning strategies. As a foundation of this research study, we will use the Conservation of Resources (COR) theory. This theory holds that the primary motivation of humans is to build, protect, and foster their resource reservoirs to protect the self and its social attachments (Hobfoll, 1998). In the context of this study, cyberslacking can be a motivation for students to manage their stress or a stress resistance (Hobfoll, 1998).

Methodology

This research study seeks to explore, via a survey instrument (Appendix A) based on a cyberslacking scale developed by Akbulut et al. (2016), this kind of behavior among dental students at the University of Puerto Rico in the Medical Sciences Campus. The study will contribute to the expansion of the cyberslacking knowledge base in the academic environment and develop new cyberslacking studies in universities after COVID-19 pandemic. The scale that will be used in the survey instrument comprised 30 items and five cyberslacking indicators, including sharing, shopping, real-time updating, accessing online content, and gaming/gambling. Students will choose their answers from offered choices, ranging from *Very unlikely* to *Very likely*. Table 1 shows every item and indicator that will be use in the survey. The study will collect data from

students in the Doctor of Dental Medicine (DMD) program and the Advanced Dental Education Programs in the School of Dental Medicine at the University of Puerto Rico, during academic years 2021-2022 and 2022-2023.

Table 1. Cyberslacking items and indicators (Akbulut et al., 2016)

No.	Statement
Sharing Items	
1	I check my friends' posts
2	I check my friends'social networking profiles
3	I share content on social networks (photo, video, etc.)
4	I like posts that are interesting
5	I comment on shared photos
6	I post status updates on social networks
7	I tag friends on photos
8	I chat with friends
9	I watch shared videos
Shopping Items	
10	I shop online
11	I visit deal-of-the-day websites
12	I visit online shopping sites
13	I visit auction sites
14	I use online banking services
15	I visit online shops for used products
16	I check job advertisements
Real-time updating Items	
17	I retweet a tweet I like
18	I favorite a tweet I like
19	I post tweets
20	I read tweets

21	I comment on trending topics
Accessing Online Content Items	
22	I download music
23	I watch videos online
24	I listen to music online
25	I download videos
26	I download applications I need
Gaming/Gambling Items	
27	I visit betting sites
28	I bet online
29	I check online sports sites
30	I play online games

Results

Once we finalize the results of this work-in-progress research study, we are expecting to have a better understanding on how cyberslacking affect student's academic progress. Also, it is our hypothesis that a high amount of students will self-admit their cyberslacking activities.

References

Akbulut, Y., Dursun, Ö. Ö., Dönmez, O., & Şahin, Y. L. (2016). In search of a measure to investigate cyberloafing in educational settings. *Computers in Human Behavior*, *55*, 616–625.

Anandarajan, M., Devine, P., & Simmers, C. A. (2004). *A multidimensional scaling approach to personal web usage in the workplace. In M. Anandarajan, & C. A. Simmers (Eds.), Personal web usage in the workplace: A guide to effective human re- source management (pp. 61–79)*. Hershey, PA: Information Science Publishing.

Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, *24*(3), 1067–1084.

Gerow, J.E., Galluch, P.S., & Thatcher, J.B. (2010). To slack or not to slack: Internet usage in the Classroom. *Journal of Information Technology Theory and Application*, *11*(3), 5-24.

Hobfoll, S. E. (1998). *Stress, culture, and community: The psychology and philosophy of stress.* Plenum Press. https://doi.org/10.1007/978-1-4899-0115-6

Junco, R., & Cotton, S.R. (2012). No A 4 U: The relationship between multitasking and academic performance. *Computers & Education*, *59*(2), 505-514.

McCoy, B.R. (2016). Digital distractions in the classroom phase II: Student classroom use of digital devices for non-class related purposes. *Journal of Media Educ*ation, *7*, 5–32.

Margaretha, M., Sherlywati, Monalisa, Y., Mariana, A., Junita, I., Martalena, Iskandar, D., & Nur. (2021). Cyberslacking behavior and its relationship with academic performance: A study of students in Indonesia. *European Journal of Educational Research*, *10*(4), 1881–1892.

Ravizza, S.M., Hambrick, D. Z., & Fenn, K.M. (2014). Non-academic Internet use in the classroom is negatively related to classroom learning regardless of intellectual ability. *Computers & Education*, *78*, 109–114.

Rosen, L. D., Lim, A. F., Carrier, L. M., & Cheever, N. A. (2008). An empirical examination of the educational impact of text message-induced task switching in the classroom: educational implications and strategies to enhance learning. *Psicología Educativa*, *17*(2), 163–177.

Sana, F., Weston, T., & Cepeda, N. J. (2013). Laptop multitasking hinders classroom learning for both users and nearby peers. *Computers & Education*, *62*, 24–31.

Simanjuntak, E., Fardana, N., & Ardi, R. (2019). Do students really use Internet access for learning in the classroom?: Exploring students'cyberslacking in an Indonesian University. *Behavioral Sciences Journal*, *9*(12), 123.

Varol, F., & Yıldırım, E. (2017). Cyberloafing in higher education: Reasons and suggestions from students' perspectives. *Technology, Knowledge, and Learning*, *24*, 129–142.

Wang, Z., David, P., Srivastava, J., Powers, S., Brady, C., D'Angelo, J., & Moreland, J. (2012). Behavioral performance and visual attention in communication multitasking: a comparison between instant messaging and online voice chat. *Computers in Human Behavior*, *28*(3), 968–975.

Wu, J., Mei, W., & Ugrin, J.C., (2018). Student cyberloafing in and out of the classroom in China and the relationship with student performance. *Cyberpsychology, Behaviour, and Social Networking*, *21*(3), 199–204.

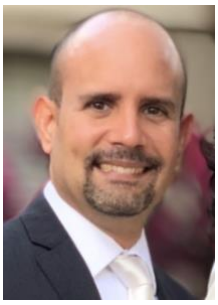
Wu, J. Y. (2017). The indirect relationship of media multitasking self-efficacy on learning performance within the personal learning environment: Implications from the mechanism of perceived attention problems and self-regulation strategies. *Computers & Education*, *106*, 56–72.

Whitty, M. T., & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behavior in the workplace. *Computers in Human Behavior*, *22*, 235-250.

Yılmaz, R., & Yurdugul, H., (2018). Cyberloafing in IT classrooms: Exploring the role of the

psycho-social environment in the classroom, attitude to computers and computing courses, motivation and learning strategies. *Journal of Computing in Higher Education*, *30*(3), 530–552.

Authors Biographies



Eliel Melón - Ramos, Ph.D. is an Associate Professor and the Director of the Center of Informatics and Educational Resources of the School of Dental Medicine in the Medical Sciences Campus at the University of Puerto Rico. He holds a Ph.D. in Information Systems from the College of Engineering and Computing from Nova Southeastern University. He also holds a Master in Business Administration with a concentration in Technology Management and a Bachelor's of Science degree in Computational Mathematics from the University of Puerto Rico at Humacao Campus. In 2019, he obtains a certification in Data Science from the University of Puerto Rico and in 2021, he completed 30 credits to obtain a Certificate in Theology at the program of Growing and Walking in the Word at the University of Leadership & Ministry. He has worked in the technology industry for more than 20 years, holding several positions including Associate Director of IT, Network Administrator and Database Administrator. Dr. Melon's research interests include Cybersecurity, Social Networks in e-learning systems, social engineering awareness, cyber threat prevention, privacy in Information Systems, Health Informatics, among others. He has taught several courses that include: Health Information Systems, Analysis, Design and Development of Health Information Systems, Introduction to Computers and Microcomputers applied to Health Sciences. He has published several academic papers in different journals like the Online Journal of Applied Knowledge Management, Issues in Information systems (IIS) Journal and in different proceedings. Also, he has served as a reviewer in several conferences like IEEE SoutheastCon for the last 6 years, KM Conference 2014-2021, IACIS 2016 and the 33rd Annual Research and Education Forum in the Medical Sciences Campus.

Wilnelia Hernández-Castro, Ph.D. In 2016 she received her Ph.D. in Information Systems from the College of Engineering and Computing at Nova Southeastern University. She also holds a Master in Business Administration with a concentration in Technology Management and a Bachelor's of Science degree in Computational Mathematics from the University of Puerto Rico. In 2019, she obtains a certification in Data Science from the University of Puerto Rico and in 2021, she completed 30 credits to obtain a Certificate in Theology at the program of Growing and Walking in the Word at the University of Leadership & Ministry. She has worked in the technology industry for more than 18 years, holding several positions including Director of Information Systems at Universidad Ana G. Méndez in Puerto Rico, a professor position at National University College in Puerto Rico and Official of Technology at the Office of Government Ethics of Puerto Rico. She has taught several courses that include: Ethics and Technology and Public Administration in the Digital Age. Dr. Hernandez's

research interests include Cyberslacking, Ethics in Computer Science, Cybersecurity, Privacy in Information Systems, among others. She has published several academic papers in different journals like the Online Journal of Applied Knowledge Management, Issues in Information systems (IIS) Journal and in different proceedings. Also, she has served as a reviewer in several conferences including IEEE SoutheastCon 2015-2018, International Association for Computer Information Systems-IACIS Europe Conference 2020, and Knowledge Management Conference 2014-2021.

Appendix A - Proposed Student's Survey

Dear student,

Please provide your self-evaluation on the following set of statements based on your behavior experience during an online class.

No.	Statement	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
Sharing Items (a)								
1a	I check my friends' posts							
2a	I check my friends' social networking profiles							
3a	I share content on social networks (photo, video, etc.)							
4a	I like posts that are interesting							
5a	I comment on shared photos							
6a	I post status updates on social networks							
7a	I tag friends on photos							
8a	I chat with friends							
9a	I watch shared videos							
Shopping Items (b)								
10b	I shop online							
11b	I visit deal-of-the-day websites							
12b	I visit online shopping sites							

13b	I visit auction sites							
14b	I use online banking services							
15b	I visit online shops for used products							
16b	I check job advertisements							
Real-time updating Items (c)								
17c	I retweet a tweet I like							
18c	I favorite a tweet I like							
19c	I post tweets							
20c	I read tweets							
21c	I comment on trending topics							
Accessing online content Items (d)								
22d	I download music							
23d	I watch videos online							
24d	I listen to music online							
25d	I download videos							
26d	I download applications I need							
Gaming/Gambling Items (e)								
27e	I visit betting sites							
28e	I bet online							
29e	I check online sports sites							
30e	I play online games							

Demographic Information

1. What is your gender?
    a. Male
    b. Female
    c. Prefer not to answer
2. What is your age group?
    a. 18 or under
    b. 19 to 24
    c. 25 to 29
    d. 30 to 34
    e. 35 to 39

   f. 40 to 44
   g. 45 to 54
   h. 55 to 59
   i. 60 or older
3. What is your highest educational degree attained?
   a. Associates degree
   b. Bachelor's degree
   c. Master's degree
   d. Professional degree
   e. Doctoral degree
4. At this moment, in what program are you enrolled in the School of Dental Medicine at the University of Puerto Rico?
   a. Doctor of Dental Medicine (DMD)
   b. Advanced Placement Program (International)
   c. General Practice Residency in Dentistry
   d. Oral and Maxillofacial Surgery
   e. Orthodontics
   f. Pediatric Dentistry
   g. Prosthodontics
5. What is your current GPA group?
   a. 3.50 - 4.00
   b. 2.50 - 3.49
   c. 1.50 - 2.49
   d. 0.00 - 1.49

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2022 – Ljubljana, Slovenia

A Publication of the International Institute for Applied Knowledge Management

An assessment of small to medium-sized enterprises' security posture and preparedness to respond to a cybersecurity attack

Stephen Mujeye, Illinois State University, USA, smujey1@ilstu.edu

[Research-in-Progress]

Abstract

Small to Medium-sized Enterprises (SMEs) play an integral role in developed countries like the United States. SMEs significantly contribute to the overall Gross Domestic Product (GDP). The number of cybersecurity attacks has been on the rise for a while. SMEs', unfortunately, have historically not been able to effectively respond to cybersecurity attacks like Fortune 500 companies and are losing revenue because of the negative consequences. SMEs have limited resources and insufficient training to thwart cybersecurity attacks. Nearly half of all cybersecurity attacks target SMEs. Therefore, this study seeks to assess SMEs' security posture and preparedness to respond to a cybersecurity attack before and after a security awareness training. A purposive sample of SMEs in central Illinois will be identified for this study. A pretest survey will be administered to individuals responsible for managing information technology at the identified SMEs. The survey questions were selected from the five functions of identity, protect, detect, respond, and recover in the National Institute for Standards and Technology (NIST) Cybersecurity Framework. That will be followed by cybersecurity training. Raising awareness through training has proved to be helpful in changing behavior. Evidence-based cybersecurity training will be offered to personnel responsible for managing information technology operations at the SMEs. The training modules will also cover the same functions in the NIST Cybersecurity Framework. A posttest survey will be administered after the training. The data will be analyzed using the multivariate analysis of variance. In this work-in-progress study, we seek to reveal if differences exist in the SMEs' ability to identify risks on assets, protect critical infrastructure, detect cybersecurity events, respond to detected cybersecurity events, and recover impaired services before and after the training. The results will help recommend the benefits of assessing an organization's security posture and training effects.

Keywords: Cybersecurity, SMEs, security training, cyber-attacks, data breaches

Introduction

In most developed countries, Small to Medium-sized Enterprises (SMEs) make up the majority of the companies. Rawindaran et al. (2021) submitted that SMEs comprise 99.9% of the six million organizations in the United Kingdom (UK). SMEs contribute nearly 50% of the United States

(U.S.)'s Gross Domestic Product (GDP). In Canada, SMEs created 77% of new private-sector jobs. SMEs make up a significant part of the economies of the U.S., Canada, the UK, and the world economy. SMEs are considered to be the backbone of the European and American economies. The U.S. Small Business Administration defined an SME as an organization with 500 or fewer employees. Marett and Barnett (2019) pointed out that SMEs do not adequately address the vulnerabilities associated with information security breaches. Consequently, SMEs have insufficient resources to develop and grow efficient security systems, limiting their access to information and guidance on business practices, including data security. SMEs lack internal expertise when compared with Fortune 500 corporations (van Haastrecht, 2021). Unlike large organizations, SMEs often lack designated security professionals to lead them against security attacks. Due to limited resources, SMEs find it impractical to hire internal security experts. Benz and Chatterjee (2020) concur that SMEs are the most vulnerable to cybersecurity risks, and their cybersecurity preparedness is subpar. More than half of the SMEs lack an up-to-date cyber risk strategy, while those leading Information Technology (IT) operations are not sure where to start to improve the security posture.

Theoretical Framework

Gafni and Pavel (2019) mentioned that SMBs in Western countries make up over 90% of companies. They also pointed out that SMBs are not always aware of attacks against their systems. Furthermore, SMBs do not often report cybersecurity attacks to law enforcement officials, and during the times they report, they are not given the same media coverage given to larger organizations. The field of IT has been revolutionized by Industry 4.0. IBM refers to Industry 4.0 as integrating new technologies such as the Internet of Things (IoT), cloud computing and analytics, artificial intelligence, and machine learning into business operations (IBM, 2022). While the implementation of Industry 4.0 initially focused on large enterprises, recently, the focus has targeted SMEs (Emer et al., 2021). SMEs have been faced with the need to protect their systems against increasing virtual and digital threats while dealing with the advancing digital transformation of Industry 4.0. With the ever-increasing number of cyberattacks, SMEs face a severe challenge in keeping their data safe and secure (Rawindaran et al., 2021). SMEs in the U.S. face more cyber-attacks than any other country, as shown in Figure 1. Raineri and Resig (2020) conducted a study that evaluated the effects of cybersecurity training on people who were attending a full-day Fall CyberSecurity Entrepreneurship Conference. Their study focused on the attendees' self-efficacy toward cybersecurity practices for small businesses. Small businesses were targeted because they are easy victims of cyberattacks because of limited resources and insufficient training. Even though small businesses suffer from several attacks such as denial of service, phishing, vishing, and data theft, small business owners lack preparedness as they falsely think their companies will not be victims. Raineri and Resig (2020) further noted that forty-three percent of cybersecurity attacks are targeted at SMEs, yet only 14% are prepared to defend their organizations. After conducting a study investigating security evaluation practices among SMEs, Moyo and Loock (2021) found out that decision-makers within SMEs have a high awareness of

the cybersecurity threats facing their organizations. Their study also found out that the decision-makers in SMEs prefer simple, user-friendly checklists and frameworks when it comes to evaluating their systems and applications. The National Institute for Standards and Technology (NIST) Cybersecurity Framework (Keller, 2021), with its five functions, provides solutions preferred by SME decision-makers.

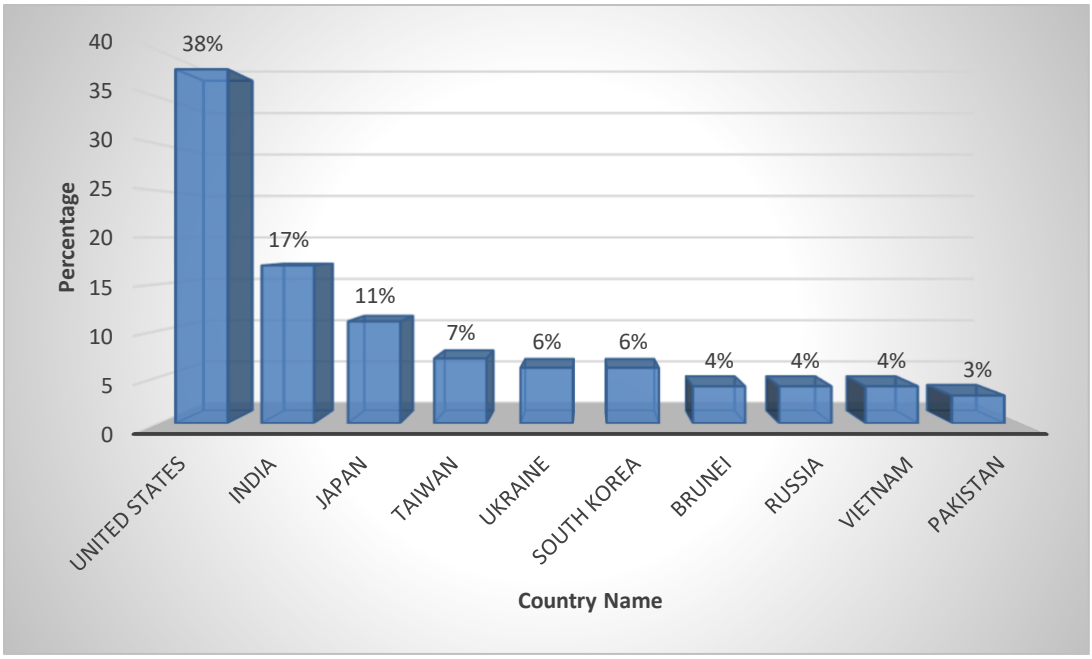


Figure 1. Cyber-attacks by Country (Adopted from Firch & Allen, 2021).

With the outbreak of COVID-19, most employees were forced to work from home. To that effect, Rawindaran et al. (2021) mentioned that challenges for SMEs increased. The Federal Bureau of Investigation (FBI) reported an increase of 300% in cybercrime since the outbreak of COVID-19 (Stouffer, n.d.). Due to the pandemic, the practice of Bring-Your-Own-Device (BYOD) has increased. SMEs can benefit from the innovations and advancements of BYOD practice. Baillette and Barlette (2018) pointed out that both employers and employees need to be aware of the risks and benefits of BYOD in SMEs. Despite the rising challenges in privacy, security, and data breaches, SMEs still need to share and exchange data. As a result of the pandemic, supply and demand shifted as some services were moved to the virtual environment. SMEs are now required to perform more and more operations in cyberspace. While SMEs have to perform more functions in cyberspace, cybercrime worldwide has also increased (Lukehart, 2022). Figure 2 shows the total cost of cybercrime globally.

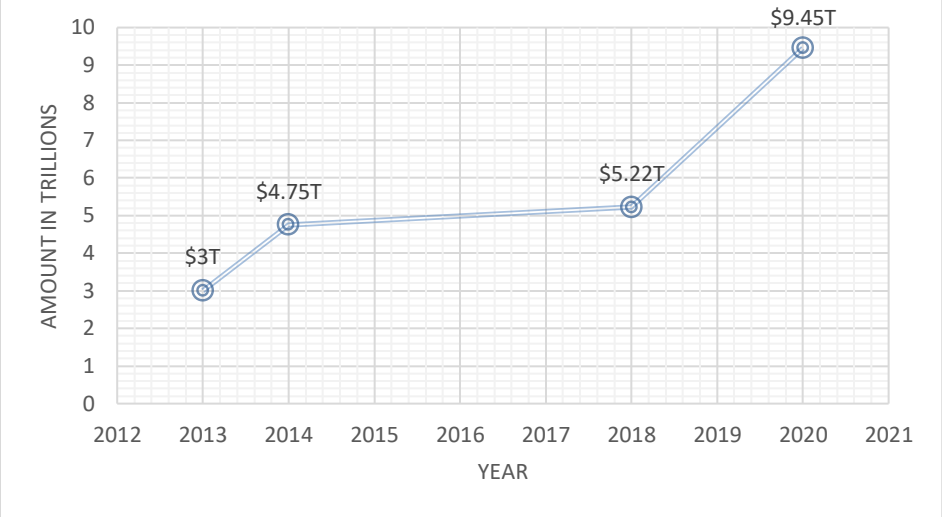


Figure 2. The Global Cost of Cybercrime (Adopted from Lukehart, 2022)

To help organizations deal with the ever-rising number of cybersecurity attacks, the NIST, a division of the Department of Commerce, took on the challenge of defending the U.S. critical infrastructure from cyber-attacks. The Cybersecurity Framework came from various IT security experts' efforts to manage risks and put remediation practices into a single coherent whole (Brumfield & Haugli, 2021). It designed the NIST Cybersecurity Framework with five functions within the Framework Core. The functions are Identify, Protect, Detect, Respond, and Recover (Keller, 2021). The *Identify* function deals with the organization's ability to identify assets that can achieve business purposes. The assets include data, personnel, devices, systems, and facilities. The cybersecurity risk assessment and a risk security management plan for the assets are defined during this function. The *Protect* function seeks to limit asset access to authorized users, processes, devices, and authorized activities. Furthermore, this function ensures that security policies, processes, and procedures are in place to manage and protect information systems and assets. In the *Detect* function, organizations have the purpose of detecting anomalous activities promptly. The impact of the anomalies and events is also understood. After anomalies are detected, the *Respond* function has a coordinated plan to respond. The response plan involves internal and external stakeholders. The function also includes a plan to prevent the expansion of any event. The last function of *Recovery* ensures that recovery processes and procedures are implemented in a way that restores affected systems and assets.

Dedeke and Masterson (2019) pointed out that the NIST Cybersecurity Framework was designed for adoption by organizations in the private and public sectors. Additionally, the framework can be used by SME decision-makers in implementing cybersecurity strategies and fighting cybersecurity attacks. The five functions were designed to protect organizations, including SMEs. As a solution for SMEs to cyberattacks, Lopez et al. (2020) pointed out that intelligent security systems capable of detecting attacks and recovering systems from the attacks are necessary. To

that end, Lopez et al. (2020) proposed a proactive security solution that incorporates machine learning and blockchain. The proposed detection system can help SMEs prevent their systems from being attacked while identifying harmful activities and stopping them from taking effect.

Methodology

A pretest-posttest training survey will be used to assess the security posture and preparedness of SMEs to respond to a cybersecurity attack. The first step will be identifying SMEs in central Illinois. The SMEs will be used as the sample in this study. SMEs are any organizations with 500 or fewer employees. The McLean County Chamber of Commerce membership directory will be used to select 50 SMEs randomly. The SMEs will be selected from the following industries: restaurant and food service; hospitality; healthcare; manufacturing; automotive, repair, and maintenance; retail; and landscaping. Contact will be made with the person responsible for managing and maintaining the IT infrastructure at the SME.

Instrumentation and Measurements

A survey will be administered to the SMEs' IT personnel at two intervals. The survey consists of 40 questions. The survey questions were selected from the five functions and subcategories in the NIST Cybersecurity Framework (Keller, 2021). The five functions and subcategories are noted in Table 1.

Table 1. The Five Functions of the NIST Cybersecurity Framework (Keller, 2021)

Identify	Protect	Detect
✓ Access management ✓ Business management ✓ Governance ✓ Risk Assessment ✓ Risk Management Strategy	✓ Access control ✓ Awareness and training ✓ Data security ✓ Information protection processes and procedures ✓ Maintenance ✓ Protective technology	✓ Anomalies and events ✓ Security continuous monitoring ✓ Detection processes

Respond	Recover
✓ Response planning ✓ Communications ✓ Analysis ✓ Mitigation ✓ Improvements	✓ Recovery planning ✓ Improvements ✓ Communications

Both the pretest and posttest surveys will be distributed via email, and they will be completed online using Qualtrics. The pretest survey will be distributed before conducting a training. The results will be recorded and will be used as a baseline. Each question will be rated on a five-point rating scale, as shown in Table 2.

Table 2. Score to numerical translation

Numerical Value	Score	Criteria for rating
1	Non-Effective Performer	The organization does not perform this function
2	Minimally Effective Performer	Not formalized and reactive
3	Effective Performer	Approved, but not implemented
4	Highly Effective Performer	Approved and partly implemented
5	Exceptional Performer	Proactively adapts function

The numeric score for each question based on the criteria ranging from "1" being a non-effective performer to "5" being exceptional performers will be recorded.

Training

Training on the subject of securing cybersecurity infrastructure will be performed with all the people who handle IT operations at the SMEs. The training will also cover all the five functions in NIST Cybersecurity Framework. The training will be scheduled either face-to-face or virtual using Zoom. The training will be done once a month for six months. The evidence-based training method will be used; this has proven effective in changing cybersecurity behaviors (He, et al., 2020). The training modules will cite sources with cybersecurity data analysis, cybersecurity observations, and cybersecurity reports. Malware attacks, including ransomware and recent data breaches, will be included in the training modules, thus making them self-relevant. The training modules will be in tangent with business processes and everyday activities. Relevant information from the five functions of NIST Cybersecurity Framework Core will be included in all the training modules. The functions to be covered are identify, protect, detect, respond, and recover. The topics of data security, common risks and vulnerabilities, accessing work systems, and password management will be covered during the training (Goode et al., 2018). After the training for six months, the posttest survey will be administered. Results will be analyzed to see if there is a difference in responses before and after the training.

Problem Statement, Goals, and Hypotheses

This research aims to assess SMEs' cybersecurity posture and preparedness to respond to a cybersecurity attack before and after a security awareness training. He (2019) pointed out that cybersecurity awareness training helps prevent security data breaches to intellectual capital. Precisely, evidence-based cybersecurity training methods have proven to be more effective. Previous studies have shown evidence-based training to have a considerable impact on the

behaviors of employees. Liu (2020) also mentioned that employee training plays a significant role in meeting information systems security policies compliance. Furthermore, Vasileiou and Furnell (2019) noted that education and raising awareness within an organization reduce insider threats. The NIST Cybersecurity Framework has been accepted and adopted widely as an approach to facilitate cybersecurity risk management in organizations (Gordon, Loeb, & Zhou, 2020). Based on the NIST Cybersecurity Framework functions, prior research, and the author's ongoing work in this area, the following hypotheses will guide this study (noted in null layout):

H1 There will be no significant differences in the SMEs' ability to *identify* risks on assets after security awareness training.

H2 There will be no significant differences in the SMEs' ability to *protect* critical infrastructure services after security awareness training.

H3 There will be no significant differences in the SMEs' ability to *detect* cybersecurity events after security awareness training promptly.

H4 There will be no significant differences in the SMEs' ability to *respond* to detected cybersecurity events after security awareness training.

H5 There will be no significant differences in the SMEs' ability to *recover* impaired services due to a cybersecurity event after security awareness training.

After the surveys have been completed, a pre-analysis data screening will be performed. Pre-analysis will help to increase the validity and accuracy of the results. SPSS Mahalanobis Distance analysis will be used to identify any outliers in the data. The pretest and posttest survey results from the SMEs will then be analyzed using the Multivariate ANalysis Of VAriance (MANOVA). The MANOVA test will be used in analyzing the hypotheses H1 through H5. MANOVA will be used because of its ability to assess differences before and after the training. The researcher will analyze the mean and standard deviation for each function.

Conclusions

This work-in-progress research seeks to assess SME's security posture and preparedness to respond to a security attack. A pretest survey will be administered before conducting security awareness training. A pos-test will be distributed after the six months of security awareness training. The data collected from the pretest and posttest will be analyzed for differences. The SMEs will be selected from businesses in central Illinois. The data analysis will help find the differences in the SMEs' ability to identify risks on assets, protect critical infrastructure, detect cybersecurity events, respond to detected cybersecurity events, and recover impaired services before and after the training. After completing the research study, the findings as they relate to the hypothesis will be recorded.

Acknowledgment

I would like to thank the anonymous referees for their careful review and valuable suggestions.

References

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors, 21*(20), 6901. https://doi.org/10.3390/s21206901

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. *Journal of Organizational Change Management, 31*(4), 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Brumfield, C., & Haugli, B. (2021). *Cybersecurity risk management: Mastering the fundamentals using the NIST Cybersecurity Framework*. John Wiley & Sons, Inc.

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information and Computer Security, 27*(3), 373–392. https://doi.org/10.1108/ICS-10-2018-0122

Emer, A., Unterhofer, M., & Rauch, E. (2021). A cybersecurity assessment model for small and medium-sized enterprises. *IEEE Engineering Management Review, 49*(2), 98–109. https://doi.org/10.1109/EMR.2021.3078077

Firch, J., & Allen, J. (2021, October 28). *10 cyber security trends you can't ignore in 2021*. PurpleSec. https://purplesec.us/cyber-security-trends-2021/

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *The Online Journal of Applied Knowledge Management, 7*(1), 14–26. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *The Online Journal of Applied Knowledge Management, 6*(1), 67–80. https://doi.org/10.36965/OJAKM.2018.6(1)67-80

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity (Oxford)*, 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21(2), 203–213. https://doi.org/10.1108/JIC-05-2019-0112

IBM (2022). How Industry 4.0 technologies are changing manufacturing. https://www.ibm.com/topics/industry-4-0

Keller, N. (2021, December 14). *Framework documents*. NIST. https://www.nist.gov/cyberframework/framework

Liu, C., Wang, C., Wang, H., & Niu, B. (2020). Influencing factors of employees' information systems security police compliance: An empirical research in China. *E3S Web of Conferences*, 218, 04032. https://doi.org/10.1051/e3sconf/202021804032

Lopez, M. A., Lombardo, J. M., López, M., Alba, C. M., Velasco, S., Braojos, M. A., & Fuentes-García, M. (2020). intelligent detection and recovery from cyberattacks for small and medium-sized enterprises. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 55–62. https://doi.org/10.9781/ijimai.2020.08.003

Lukehart, A. (2022, January 5). *2021 Cyber attack statistics, data, and trends*. Parachute. https://parachutetechs.com/2022-cyber-attack-statistics-data-and-trends/

Marett, K., & Barnett, T. (2019). Information security practices in small-to-medium sized businesses: A hotspot analysis. *Information Resources Management Journal*, *32*(2), 76–93. https://doi.org/10.4018/IRMJ.2019040104

Moyo, M., & Loock, M. (2021). Conceptualising a cloud business intelligence security evaluation framework for small and medium enterprises in small towns of the Limpopo Province, South Africa. *Information*, *12*(3), 128. https://doi.org/10.3390/info12030128

Pagura, I. (2020). Small business and cyber security. *Journal of the Australian Traditional-Medicine Society*, *26*(1), 38–39.

Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *The Journal of Applied Business and Economics*, *22*(12), 13-23.

Rawindaran, J., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

Rothwell. (2005). External validity of randomised controlled trials: "To whom do the results of this trial apply?" *The Lancet (British Edition)*, 365(9453), 82–93. https://doi.org/10.1016/S0140-6736(04)17670-8

Sen, J. R. (2020). Strong cybersecurity strategy not a luxury for small business. *The Idaho Business Review*.

Stouffer, C. (n.d.). *115 cybersecurity statistics and trends you need to know in 2021*. Norton. https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Brinkhuis, M., & Spruit, M. (2021). *A shared cyber threat intelligence solution for SMEs. Electronics*, *10*(23), 2913. https://doi.org/10.3390/electronics10232913

Vasileiou, I., & Furnell, S. (2019). Cybersecurity education for awareness and compliance. *IGI Global.* https://doi.org/10.4018/978-1-5225-7847-5

Author's Biography

Dr. Stephen Mujeye an Assistant Professor of Computer Systems Technology at Illinois State University, Normal, Illinois. He earned a bachelor's degree with a double major in Business Management and Business Systems Support Specialist from Siena Heights University, Adrian, Michigan. He has a master's degree in Information Resource Management from Central Michigan University, Mt. Pleasant, Michigan. He completed his Ph.D. in Information Systems from Nova Southeastern University. His Ph.D. dissertation was titled "An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity.*"* He holds several industry certifications, including A+, Network+, CCNA, and CCNA Security. His areas of research interest are authentication methods, cybersecurity, as well as mobile and network security.