Refereed Proceedings - Abstracts

Sponsors:

HfTL

Hochschule für Telekommunikation Leipzig
University of Applied Sciences

International Institute for Applied
Knowledge Management

NOVA SOUTHEASTERN
UNIVERSITY
NSU
Florida

Additional Conference Sponsors:

Platinum Support
Anonymous (5x)
Dr. Boštjan Delak
Dr. Molly Cooper

Silver Support
Dr. Eliel Melon
Dr. Wilnelia Hernandez-Castro

Table of Contents

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

KM2021 Conference Co-Chairs

Oliver Jokisch	Vered Silber-Varod
HfTL University Leipzig, Germany	The Open University of Israel, Israel
jokisch@hft-leipzig.de	vereds@openu.ac.il

KM2021 Local Conference Organizers and Coordinators

Gunnar Auth	Ingo Siegert	Joanna Santiago
HSF University of Applied Sciences, Germany	Otto-von-Guericke University, Germany	ISEG - University of Lisbon, Portugal
Gunnar.Auth@hsf.sachsen.de	ingo.siegert@ovgu.de	joannas@iseg.ulisboa.pt

KM2021 Conference Organizers and Coordinators

Yair Levy Nova Southeastern University, FL, USA levyy@nova.edu	Shonda Brown Middle Georgia State University, USA Shonda.Brown@mga.edu	Michelle M. Ramim Nova Southeastern University, USA michelle.ramim@gmail.com	Nathan White Central Washington University, USA nathan.white@cwu.edu

KM2021 Conference Workshops Co-Chairs

Boštjan Delak	Celina Sołek-Borowska
Faculty of Information studies, Slovenia	Warsaw School of Economics, Poland
bostjan.delak@fis.unm.si	csolek@sgh.waw.pl

KM2021 Program Committee Co-Chairs

Nitza Geri	Jean-Henry Morin	Melissa Carlton
The Open University of Israel, Israel	University of Geneva, Switzerland	Houston Baptist University, USA
nitzage@openu.ac.il	Jean-Henry.Morin@unige.ch	mcarlton@hbu.edu

KM2021 Program Committee Members

Gunnar Auth	HSF University of Applied Sciences, Germany
Dizza Beimel	Ruppin Academic Center, Israel
Ofir Ben Assuli	Ono Academic College, Israel
Ina Blau	The Open University of Israel, Israel
Carlene Blackwood-Brown	Seneca College, Canada
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
Fatih Çetin	Nigde Ömer Halisdemir University, Turkey
Witold Chmielarz	University of Warsaw, Poland
Dimitar Christozov	American University of Bulgaria, Bulgaria
Malgorzata Cieciora	Polish-Japanese Academy of Information Technology, Poland
Molly Cooper	Ferris State University, USA
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
Yoram Eshet-Alkalai	The Open University of Israel, Israel
Ruti Gafni	Tel-Aviv Yaffo Academic College, Israel
Michal Golinski	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	Leipzig University of Telecommunications (HfTL), Germany
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
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
Paula Peres	Polytechnic Institute of Porto, Portugal
Michal Pietrzak	Warsaw University of Life Sciences, Poland

Margarida Piteira	ISEG - University of Lisbon, Portugal
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
Gilad Ravid	Ben Gurion University of the Negev, Israel
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
Tamar Shamir-Inbal	The Open University of Israel, Israel
Ingo Siegert	Otto von Guericke University, Germany
Marcin Sikorski	Gdansk University of Technology, Poland
Vered Silber-Varod	The Open University of Israel, Israel
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
Amir Winer	The Open University of Israel, Israel
Jedrzej Wieczorkowski	Warsaw School of Economics, Poland
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!

Adding knowledge to your data: Enterprise knowledge graph management with eccenca corporate memory

[Industry Keynote]

Sebastian Tramp, eccenca GmbH, Leipzig, Germany, sebastian.tramp@eccenca.com

Abstract

Knowledge Graph Management plays an increasing role in modern enterprise applications. eccenca Corporate Memory provides a multi-disciplinary integrative platform for managing rules and constraints and data in a single application. Overcoming the limitations of traditional, application centric (meta) data management models, its semantic knowledge graph is both highly extensible, integrative as well as interpretable both by machines and business users. In this talk, Sebastian will give an overview on the capabilities of eccenca Corporate Memory as well as describe best practices and processes on how to add knowledge to your data to enable smart decision making and automation.

Language interfaces with automated components for business applications

[Industry Invited Talk]

Andreas Niekler, Institute of Computer Science at Universität Leipzig, Germany, aniekler@informatik.uni-leipzig.de

Abstract

Language interfaces play an increasing role in modern business applications. We show the outline of an integration of unstructured data and Robotic Process Automation (RPA) approaches into a chatbot framework. We describe how RPA applications are connected to a chatbot system and show a possible system sketch. Furthermore, we describe the integration of Open Question Answering techniques like DocChat, semantic clustering and the Universal Sentence Encoder in order to acquire direct answers to user questions from documents. We also show a standalone bot framework product of 1000° Digital GmbH for deployment in industrial contexts.

Digital transformation for the German energy transition – developing a centralized knowledge management database for the energy market

[Industry Invited Talk]

Florian Marquardt, Regiocom SE Magdeburg, Germany, florian.marquardt@regiocom.com

Abstract

The corporation Regiocom SE is an international service provider for contact center services and process digitization related to the energy market. The German energy transition accompanies a process in which once manageable numbers of energy-generating and feed-in plants, primarily large-scale power plants for coal, gas, water, and nuclear energy, are being supplemented and partially subsumed by more and more small decentralized units, such as solar plants, CHP plants, wind turbines but also stationary battery storage and emergency generators. Issues such as grid expansion but also operational grid control require the actual and correct availability of unanimous master data for these plants. Currently, more than two million power plants are feeding into the German energy grid, which have to be synchronized in future to prevent blackouts or critical shortages. On behalf of the Federal Network Agency, Regiocom has designed, implemented, and put into operation a nationwide Core energy market data register (MaStR). Since the beginning of 2019, this system has provided a central database for all energy-generating plants, based on which it has been possible to develop value-added services for industry and research. Details about the development, the actual status and possible use cases only possible with this centralized knowledge will be presented in the talk.

How do we increase and optimize the degree of information and knowledge reuse at CORE?

[Industry Invited Talk]

Evgeniya Ivanova, CORE SE Consultancy, Germany, evgeniya.ivanova@core.se

Abstract

CORE is a Technology Think Tank and accompanies the management of complex technology transformations of institutions in which IT constitutes a disproportionately high contribution factor to business success. Based on detailed market knowledge, in-depth technology expertise and high methodological competence, CORE SE develops solutions, securing the sustainability of the clients' value chains. Some companies have lack of awareness and knowledge what are the knowledge sharing mechanisms in the organizations and what are their strategic business outcomes and effects today. As a trusted partner for start-ups, fintechs, universal banking and governmental institutions, especially in highly regulated industries such as finance, biotech, automotive and aviation, CORE recognizes the need of strong knowledge management that is based on the organization, modern technology and corporate culture and helps to expand and to develop company's core competences and to strengthen market position and industry competitiveness. Only by reusing existing knowledge and methodologies, supported by technology and employee values, is it possible to transform a company to the learning organization in which knowledge plays a crucial role in achieving strategic goals.

Setup and knowledge sharing of the new Fraunhofer research group for cognitive material diagnostics

[Industry Invited Talk]

Ivan Kraljevski, Fraunhofer IKTS and Brandenburg University of Technology, Germany, ivan.kraljevski@ikts.fraunhofer.de

Abstract

The value and the ability to manage knowledge are essential assets required for any business decisions in an organization. Data mining and analysis derive valuable knowledge, which is more accessible, interpretable, actionable and provides more distilled insights. However, often knowledge discovery is difficult due to the nature of the industrial and business processes. Therefore, employing artificial intelligence in the creation, consumption, and sharing of knowledge could provide tailored and automated solutions for enterprises. The Fraunhofer IKTS project group “Cognitive Material Diagnostics” (KogMatD) in Cottbus aims to address these challenges by developing intelligent systems based on artificial intelligence and machine learning for discovering and sharing relevant knowledge derived from material diagnostics. Rapid transfer of the research results into applications with social relevance is the objective of the interdisciplinary team of experts. Deployment of practical solutions in the early stage supports business processes from virtual product development to comprehensive automation and networking. By choosing Cottbus as its site in the “Lausitz” region, Fraunhofer IKTS demonstrates its social responsibility by bringing excellence in applied research to structurally weak regions. The development of research activities in the mining region envisioned creating new qualified and forward-looking jobs in cognitive materials, machine learning, and artificial intelligence.

Cybersecurity – Do we have the knowledge to manage it?

[Keynote]

Steven Furnell, University of Nottingham, United Kingdom, Steven.Furnell@nottingham.ac.uk

Abstract

Cybersecurity is now regularly encountered by IT users in both personal and workplace contexts. However, despite widespread and established use of digital technology, our ability to use it in a security- aware manner is arguably lagging behind our enthusiasm for deploying devices and adopting new services. This leads to recognised problems in terms of user-focused threats and exploitation, but the most common response is frequently to try to direct more technology toward the problem. This presentation proposes that what is actually required is a credible foundation of cybersecurity literacy, sitting within the wider context of digital/data literacy frameworks. The discussion considers what ought to be encompassed within such an approach, including to ensure that users have credible knowledge and understanding of the threats they may face and the safeguards to protect against them, alongside the skills and capabilities to put such knowledge into practice. At the same time, there are challenges to be faced in terms of how to promote and provide the required knowledge, and the consistency of information that users may receive. There is also the overarching challenge of an ever-broadening range of devices and services to which such knowledge needs to be applied, as well as the evolving landscape of threats and safeguards as further new technologies and applications continue to emerge.

Knowledge transfer: Leveraging human predispositions for explaining and understanding

[Keynote]

Britta Wrede, Medical School OWL and Center for Cognitive Interaction Technology, Bielefeld University, Germany, bwrede@techfak.uni-bielefeld.de

Abstract

One of the characteristics that sets humans apart from other species is their ability and predisposition to transfer knowledge to their offspring. Research in developmental psychology shows how parents as tutors make use of a range of strategies to convey knowledge that would otherwise be opaque to their infants. However, it has also been shown that infants not only have a predisposition that makes them especially prone to understand such opaque knowledge but that they also play an active role in this process.

In my talk, I will give insights how to leverage these predispositions of teachers and learners for knowledge transfer between humans and machines. In the case of machines as learners, human teachers provide knowledge in a specific way that a robot can use to structure the input and filter out irrelevant information. On the other hand, through contingent behavior a robot can motivate the tutor to provide specifically well-suited input for the learner. In scenarios where machines transfer knowledge to humans, a typical task for assistive systems, they have to be specifically sensitive to human feedback in order to adapt to their understanding processes as observed through task process or facial expressions and to their attentional state as a cue of engagement and understanding. These capabilities are also basic prerequisites for a more interactive account of explainable AI as a specific and increasingly important topic of knowledge transfer.

Managing industrial and research information using knowledge graphs

[Keynote]

Sören Auer, Data Science and Digital Libraries, Leibniz Universität Hannover, Germany, auer@tib.eu

Abstract

The availability of large-scale datasets has unleashed an enormous potential of making computers smarter and gave rise to cognitive computing. In order to realize the potential of Artificial Intelligence (AI) a common understanding of the structure and meaning of data (e.g. to be used as training or evaluation data) must be established. We can leverage vocabularies, Linked Data, knowledge graphs or Semantic Data Lakes for that purpose. In this talk we give an overview on recent approaches in the area of data spaces and knowledge graphs, which all help to realize the emerging concept of hybrid AI, where large- scale, rich semantic data and knowledge tightly interacts with machine learning and analytics. We discuss some enterprise applications and present with the Open Research Knowledge Graph a use case and approach for semantically describing and organizing scientific contributions to empower researchers to master the flood of static scientific publications.

Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

A cross-language study of speech recognition systems for English, German, and Hebrew

Vered Silber Varod, Open Media and Information Lab, The Open University of Israel, Israel, vereds@openu.ac.il

Ingo Siegert, Mobile Dialog Systems, Otto von Guericke University Magdeburg, Germany, ingo.siegert@ovgu.de

Oliver Jokisch, Institute of Communications Engineering, Leipzig University of Telecommunications, Germany, jokisch@hft-leipzig.de

Yamini Sinha, Mobile Dialog Systems, Otto von Guericke University Magdeburg, Germany, yamini.sinha@st.ovgu.de

Nitza Geri, Department of Management and Economics, The Open University of Israel, Israel, nitzage@openu.ac.il

Abstract

Despite the growing importance of Automatic Speech Recognition (ASR), its application is still challenging, limited, language-dependent, and requires considerable resources. The resources required for ASR are not only technical, they also need to reflect technological trends and cultural diversity. The purpose of this research is to explore ASR performance gaps by a comparative study of American English, German, and Hebrew. Apart from different languages, we also investigate different speaking styles – utterances from spontaneous dialogues and utterances from frontal lectures (TED-like genre). The analysis includes a comparison of the performance of four ASR engines (Google Cloud, Google Search, IBM Watson, and WIT.ai) using four commonly used metrics: Word Error Rate (WER); Character Error Rate (CER); Word Information Lost (WIL); and Match Error Rate (MER). As expected, findings suggest that English ASR systems provide the best results. Contrary to our hypothesis regarding ASR's low performance for under-resourced languages, we found that the Hebrew and German ASR systems have similar performance. Overall, our findings suggest that ASR performance is language-dependent and system-dependent. Furthermore, ASR may be genre-sensitive, as our results showed for German. This research contributes a valuable insight for improving ubiquitous global consumption and management of knowledge and calls for corporate social responsibility of commercial companies, to develop ASR under Fair, Reasonable and Non-Discriminatory (FRAND) terms.

Keywords: Automatic Speech Recognition (ASR), performance measures, speech-recognition evaluation metrics, ASR engine, cross-language, genre, error rate.

Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

An examination of historic data breach incidents: What cybersecurity big data visualization and analytics can tell us?

Emily Africk, USA, eafrick@umich.edu

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

Abstract

Data breach incidents are reported in the media to be on the rise with continuously increasing numbers. Additionally, data breaches serve a major negative impact to organizations. This study focuses on combining experience in data analytics, visualization, and quantitative analysis for business intelligence in the context of cybersecurity big-data over a period of 15-years. A large data set containing 9,015 data breaches was provided via the Privacy Rights Clearinghouse data breach database from the start of 2005 to the end of 2019. The aim of this work was to slice the data as well as represent it into a business-related visualization using time-series analysis that can help executives understand complex cybersecurity breaches, their impact, and their trend over time. We have created visualization figures along with explanations of what each visualization means in the context of cyber-attacks over time. This project was set to serve as a breakdown of the important findings from the Privacy Rights Clearinghouse data breach database of over 15-years. These findings are communicated through both key numbers and quantitative analyses for business intelligence. While our project does not cover every aspect of the dataset (due to its significant size), it serves more as a focus on one particular part of the data: incident types and their volume over the 15-year timeframe to help business executives visualize cybersecurity trends. This paper ends with a conclusion and discussion on how such cybersecurity visualizations can help industries along with future research needed.

Keywords: Cybersecurity data analytics, data breach incidents, visualizations of data breaches, cybersecurity big data, time-series analysis of data breaches.

Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

Artificial intelligence for last-mile logistics – Procedures and architecture

André Rosendorff, University of Applied Sciences for Telecommunications (HfTL), Chair of Business Intelligence and Data Science, Germany, andre.rosendorff@web.de

Alexander Hodes, University of Applied Sciences for Telecommunications Leipzig (HfTL), Chair of Business Intelligence and Data Science, Germany, alexander.hodes@live.com

Benjamin Fabian, Technical University of Applied Sciences Wildau (TH Wildau), Chair of E-Government, IT-Security and IT Management, Germany, benjamin.fabian@th-wildau.de

Abstract

Artificial intelligence is gaining in importance due to the many application areas and potentials in many industries. In logistics, in particular, increasing customer requirements and the growth of shipment volumes lead to difficulties in forecasting delivery times, especially for the last mile. In this paper, the potentials of using AI to improve the delivery forecast are examined. For this goal, we provide a structured theoretical solution approach and procedure for the improvement of the delivery prognosis through Artificial Intelligence. Here, the important phases of the CRISP-DM framework, a standard process for data mining, are adopted and discussed in detail, demonstrating the complexity and importance of the individual tasks such as data preparation or evaluation. Then, by embedding the described solution into an overall information systems architecture, we provide ideas for integrating the solution into the complexity of real-world information systems for logistics.

Keywords: Supply chain management, logistics, artificial intelligence, machine learning, business intelligence.

Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

The case of savvy customers in the times of pandemic: Customers' technology savviness and social media communication impact on customer-based brand equity

Joanna Krywalski Santiago, ADVANCE, ISEG – Lisbon School of Economics and Management, Portugal, joannas@iseg.ulisboa.pt

Miguel Pimenta, ISEG – Lisbon School of Economics and Management, Portugal, l51819@aln.iseg.ulisboa.pt

Abstract

This paper follows the recent areas of interest trucked by Google Trends to investigate the importance of firm's social media communication at creation of brand equity influenced by customers' technological savviness. Additionally, this study brings some light into consumer behavior during pandemic. The data was collected through an online survey distributed in Portugal in September 2020 with the assistance of Qualtrics online survey platform and counted with 267 responses. To understand the relationships between customer technology savviness (CTS), firm's social media communication (SMC) and customer-based brand equity (CBBE), this study applies the partial last squares method of structural equation modelling (PLS-SEM). The results of the multigroup analysis show that customers who used social media more heavily during pandemic denoted a stronger relationship between CTS and CBBE, CTS and SMC and between SMC and CBBE, of which the last was not confirmed in case of customers who made less use of social media since the outbreak of COVID-19 pandemic.

Keywords: Technology savviness, social media communication, customer-based brand equity.

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

Is the "learning organization" still a good concept? A historical analysis of the LO conceptual ontogenesis

[Research-in-Progress]

Sitthimet Solthong, Bangkok University, Thailand, sitthimet@gmail.com

Xavier Parisot, IKI-SEA, Bangkok University, Thailand, xavier.p@bu.ac.th

Abstract

The terms "organizational learning" and "Learning Organization" (LO) have been used as interchangeable concepts over a long period. Even after the clarification and discrimination of these two concepts in the literature, some confusion remains. Indeed, the definitional scope of the LO concept has varied greatly over the past three decades. To confirm which Defining Attributes (DA) are at the core of the concept, 40 historical definitions have been selected from 1989 to 2018. Their DA are identified. Similar DA are grouped and their frequencies are calculated. The most frequent DA are considered to be at the core of the LO conceptual definition. Among all the analyzed definitions, one definition encompasses all these core DA. The goodness of this definition is evaluated using Gerring's eight parameter framework. The results show that the conceptualization of the LO based on its most frequent DA leads to moderate to high scores for seven parameters (familiarity, resonance, coherence, depth, differentiation, theoretical utility, and field utility) and below an average score for one parameter (parsimony). This historical approach of the LO conceptual ontogenesis allows one to discriminate between the core and the peripheral DA and therefore to refocus its definition on specific phenomena. The analysis of the relevancy of these core DA also demonstrates that the goodness of the LO concept still can be improved by removing the multiple historical changes applied to its definitions.

Keywords: Learning organization, ontology, concept formation, defining attributes, concept's goodness.

International Institute for Applied
Knowledge Management

Refereed Paper Proceedings - KM Conference 2021 – Leipzig, Germany
A Publication of the International Institute for Applied Knowledge Management

Identifying skills gaps and predicting practicum performance in a graduate program using a survey instrument designed around health informatics domains and competencies

[Research-in-Progress]

Stephen E. Bronsburg, Dr. Kiran C. Patel College of Osteopathic Medicine, Nova Southeastern University, USA, bronsbur@nova.edu

Michelle Ramim, Dr. Kiran C. Patel College of Osteopathic Medicine, Nova Southeastern University, USA, ramim@nova.edu

Abstract

The interdisciplinary field of health informatics began around the 1960s when computers were sophisticated enough to handle larger amounts of data. In 2012, the American Medical Informatic Association (AMIA) Board published a White Paper outlining health informatics core-competencies for graduate programs. Following this paper, in 2014 the AMIA and the Commission on Accreditation for Health Informatics and Information Management (CAHIIM), together revised existing health informatics curriculum requirements to three co-mingled domains: health, information science and technology, as well as social and behavioral science. This work-in-progress research will utilize these three foundational domains, and the cross academic domains (10 in total) as the basis for a newly developed survey instrument, which will be administered to graduate health informatic students prior to their final core course, the practicum. Each survey questions will be weighted in the rubric.

Keywords: Health informatics, health informatics practicum, informatics competency rubric, predicting practicum performance, knowledge flow.

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

A survey of IT professionals' perception of ransomware

[Complete Research]

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

Abstract

Ransomware is a malware attack in which cybercriminals encrypt data and demand a ransom fee for the legitimate user to regain access to electronic devices and data. Ransomware attacks have significantly increased in recent years. More and more organizations are affected by ransomware. Ransomware affects organizations in healthcare, education, governmental institutions as well as private businesses. The amount of ransom being demanded from organizations is also going up, and some organizations are reported to have paid millions of dollars. On a global scale, ransomware is expected to cost businesses more than $20 billion in 2021. In this study, a survey was used to investigate how Information Technology (IT) professionals perceive ransomware. The survey was completed by 27 IT professionals representing different organizations as well as from different positions. The survey results indicated that most IT professionals view ransomware as the current leading cybersecurity attack on information systems. They also overwhelmingly rated ransomware as being one of the deadliest types of cyber-attack. As a result of analyzing the results, it was concluded that all IT professionals believe educating regular network users can go a long way in preventing and mitigating ransomware attacks. Educating users on security risks like clicking links in emails and on text messages can help combat ransomware. There is a therefore a greater need for user education and raising awareness of behaviors that can contribute to ransomware attacks. Furthermore, backing up data and verifying the backups can help fight ransomware. Implementing good security policies was also cited as helping fight ransomware. The results of this study are useful and helpful to all cybersecurity professionals. The findings may help both organizations and individuals in the fight against the deadly ransomware attacks.

Keywords: Malware, ransomware, cybersecurity, cyberwar, security.

International Institute for Applied
Knowledge Management

Refereed Paper Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

Providing language interfaces with robotic process automation and text retrieval for automated integration of applications and unstructured data

[Research-in-Progress]

Andreas Niekler, Leipzig University, Germany, aniekler@informatik.uni-leipzig.de

Mark Busse, 1000° Digital GmbH, Germany, mark.busse@1000grad.de

Matthias Gulde, Leipzig University, Germany, mt.delgu@gmail.com

Lino Markfort, Leipzig University, Germany, lino.markfort@uni-leipzig.de

Felix Helfer, Leipzig University, Germany, helfer@informatik.uni-leipzig.de

Abstract

In this paper we show the outline of an integration of unstructured data and Robotic Process Automation (RPA) approaches into a chatbot framework. We describe how RPA applications are connected to a chatbot system and show a possible system sketch. Furthermore, we describe the integration of Open Question Answering techniques like DocChat, semantic clustering and the Universal Sentence Encoder in order to acquire direct answers to user questions from documents. From this, we derive a standalone bot framework that we will use in the future for deployment in industrial contexts. For this purpose, we integrate the tools in a user and application-oriented way in the near future.

Keywords: Chatbot, conversational interface, natural language processing, information retrieval, robotic process automation.

International Institute for Applied
Knowledge Management

Refereed Paper Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

Towards a universal cybersecurity competency framework for organizational users

[Research-in-Progress]

Patricia Baker, Nova Southeastern University, USA, patrbake@mynsu.nova.edu

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

Ling Wang, Nova Southeastern University, USA, lingwang@nova.edu

Martha Snyder, Nova Southeastern University, USA, smithmt@nova.edu

Abstract

Organizations have invested a tremendous amount of time and resources in improving their Information Security Policies (ISPs) to mitigate cyber-attacks. However, organizations continue to fall prey to data breaches, and the human factor in cybersecurity appears to be the leading cause in most cases. Additionally, despite the abundance of research conducted on cybersecurity mitigation, prior research indicated that cybersecurity competency of users is a significant cause of data breaches. The purpose of this empirical work-in-progress research is to investigate, evaluate and quantify the cybersecurity competency of users in a universal measure beyond that of Information Technology (IT) professionals. The significance of this study attempts to develop a universal scale for organizations to effectively manage users' cybersecurity knowledge, skills, and tasks (KSTs). The work-in-progress study will utilize between 30 and 50 Subject Matter Experts (SMEs) to engage in a two-phase Delphi method to validate the KSTs necessary for the universal Cybersecurity Competency Framework (CCF). The Kendall W coefficient of agreement and Spearman rho correlation of agreement will be utilized to test the level of consensus amongst the SMEs. The creation of the universal CCF will assist in categorizing users' cybersecurity competency to create organizational cybersecurity structures, thus, reducing cyber-attacks.

Keywords: Cybersecurity competency, cybersecurity workforce, cybersecurity knowledge, cybersecurity skills, cybersecurity tasks.

Faculty's perceptions of embedded librarians and OER knowledge mashups in academia

[Complete Research]

Scott Spangler, Middle Georgia State University, USA, sspangler.us@gmail.com

Dana Casper, Middle Georgia State University, USA, dana.casper@mga.edu

Deborah Stanfield, Middle Georgia State University, USA, deborah.standfield@mga.edu

Extended Abstract

In February of 2020, the COVID-19 phenomena forced colleges and universities into emergency response planning models. Inside of the models, new purposefulness academic role changes occurred. The pandemic inspired methods professors utilized to share, transfer and manage knowledge to their students fostered new innovations and collaborative adventures in academia. To foster student success and further disseminate information, faculty collaborated with the gatekeepers of knowledge at Universities–the Librarians.

Hence, the purpose of the pilot study is to evaluate faculty's perceptions of embedded librarians and their Open-Educational Resources Academic Directories (OERAD) or "mashups" of purposeful managed knowledge they share with students for success and retention in an online learning environment during the pandemic at a Southeastern public university. The data were collected through a purposeful sample (n=27) using an electronic survey instrument during an institutional disruption in library services. The study's tool and methodology are framed through prior scholars' literature with permission. The researchers obtained an Institutional Review Board (IRB)'s approval of the methodology, analysis method, and tool to increase the integrity and validation of the data.

The data were organized, administered, and processed through Google's research tools as well as SPSS statistical analysis software. The pilot study concurs with prior literature's three main constructs: comfort, confidence, and self-efficacy. It also contends that the embedded librarian's OERAD instruments or "mashups" of knowledge have value in transfer and design. Additionally, this study recognizes the need for faculty collaboration with an embedded librarian in coursework for student success. It also recognizes the need for additional research into understanding how knowledge in open-educational resources can be "mashed-up" to further its transfer, which may decrease the ever-present gap in educational resources to rural and disenfranchised students. Finally, this study acknowledges its limitations and recommendations for future research in knowledge management.

Keywords: Embedded librarian, course-integrated instruction, online instruction open educational resources.

International Institute for Applied Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

How individualistic and collectivistic cultures affect leadership of schools' ICT coordinators, digital collaboration skills of students and sustainability of e-collaboration?

[Complete Research]

Ina Blau, The Open University of Israel, Israel, inabl@openu.ac.il

Tamar Shamir-Inbal, The Open University of Israel, Israel, tamaris@openu.ac.il

Shlomit Hadad, Bar Ilan University, Israel, shsh3345@gmail.com

Extended Abstract

The purpose of this study was to examine the influence of online collaborative learning on the digital collaboration skills of students and on the sustainability of technology-enhanced collaboration in the schools' culture – individualistic versus collectivistic. In addition, the study explored how leadership experience of the schools' Information and Communication Technology (ICT) coordinators while leading the collaborative projects, was predicted by their sense of professionalism, as well as the cognitive, emotional, and social aspects of perceived learning. The participants were ICT coordinators from 513 Israeli schools, 214 of whom were Hebrew-speakers with a more individualistic culture and 299 Arabic-speakers with a more collectivistic learning culture. The ICT coordinators were asked to complete an online questionnaire, which included multiple-choice and open-ended questions. The results showed significant differences between a variety of the coordinators' characteristics as a function of differences between more individualistic versus more collectivistic learning cultures; however, students' digital collaboration skills were not affected by these differences. Students' digital skills and coordinators' cognitive and social perceived learning were significant predictors of coordinators' leadership experience in both schools with more individualistic and with more collectivistic learning cultures. Emotional perceived learning predicted learning experience of ICT coordinators only in schools with a more collectivistic learning culture. Leadership experience of ICT coordinators was a powerful predictor of students' digital collaboration skills, but did not predict the sustainability of technology-enhanced collaboration in schools. The emotional perceived learning of coordinators predicted the sustainability of technology-enhanced collaboration in both types of schools. These findings contribute to technology-enhanced learning theory and educational practice.

Keywords: Online collaborative learning, ICT school coordinators, individualistic vs collectivistic school culture, e-collaboration skills, leadership, perceived learning.

References:

Blau, I., Shamir-Inbal, T. & Hadad, S. (2020). Digital collaborative learning in elementary and middle schools as a function of individualistic and collectivistic culture: The role of ICT coordinators' leadership experience, students' collaboration skills, and sustainability. *Journal of Computer Assisted Learning, 36*(5), 672-687.

What are the characteristics of pedagogical change in integrating digital collaborative learning within and between schools?

[Complete Research]

Tamar Shamir-Inbal, The Open University of Israel, Israel, tamaris@openu.ac.il

Ina Blau, The Open University of Israel, Israel, inabl@openu.ac.il

Extended Abstract

Collaborative Learning (CL) is an important component of integrating digital technologies in schools. This study examines the initiative of the Ministry of Education ICT supervision to conduct digital collaborative projects within and between schools. The analysis was based on the conceptual framework SAMR (Puentedura, 2012), which differentiates the degree of pedagogical change in technology integration. The *SAMR* model describes four levels of change as either minor - *Substitution* and *Augmentation* - or substantial change - *Modification* and *Redefinition*. This research adds to literature by combining the analysis based on the SAMR framework with different levels of collaboration in educational context. The levels of collaboration are (Blau, 2011): information sharing - the most basic type of collaboration of making an individual learning experience, idea, or artifact accessible to others, cooperation - division of a task among the participants, and collaboration - the highest level of teamwork, which involves engagement of participants in the entire process. Further, the study analyzed collaborative learning outcomes created and presented by the students. The participants were 159 ICT leaders, who designed 37 collaborative learning activities in order to promote students' digital collaboration between schools. The qualitative study was conducted through thematic analysis of 37 digital collaborative learning activities presented on the district website. All levels of the SAMR model were present in the CL activities in our study, while the most common categories were the two middle levels - augmentation and modification. Regarding the levels of collaboration, it was found that most of the tasks reflected the cooperation level, while the higher level of teamwork was less common in projects analyzed in this study. Based on the findings, the paper offers an extension of the SAMR model that combines the level of technological-pedagogical change with levels of digital collaboration into the comprehensive e-CSAMR (e-collaboration & SAMR) framework. The implications for educational theory and practice are discussed.

Keywords: Digital collaborative learning, SAMR framework, collaboration levels, ICT school leaders, between school projects.

References:

Blau, I. (2011). E-collaboration within, between, and without institutions: Towards a better functioning of online groups through networks. *International Journal of e-Collaboration, 7,* 22-36.

Puentedura, R. (2012). *The SAMR model: Six exemplars*. http://www.hippasus.com/rrpweblog/archives/2012/08/14/SAMR_SixExemplars.pdf

Considering time in prediction of congestive heart failure events

[Research-in-Progress]

Ofir Ben-Assuli, Ono Academic College, Israel, ofir.benassuli@gmail.com

Roni Ramon, Bar Ilan University, Israel, roni.ramon@gmail.com

Tsipi Heart, Ono Academic College, Israel, tsipi.h@ono.ac.il

Arie Jacobi, Ono Academic College, Israel, jacobi.arie@gmail.com

Robert Klempfner, Sheba Medical Center, Israel, Robert.Klempfner@sheba.health.gov.il

Extended Abstract

Congestive Heart Failure (CHF) is a clinical syndrome characterized by comorbidities and adverse medical events. Medical data analytics and knowledge management influence decision-making effectiveness (Wang & Byrd, 2017). Risk prediction to identify patients most likely to die shortly after discharge is a strategy to improve the quality of care by better allocating organizational resources and personalized interventions. Currently, considering the time in predicting adverse medical events have several limitations resulting from the complexity of the medical data. The research objective is to apply prediction models that consider the time to adverse medical events, taking into account dependencies among observations. In the healthcare literature, there is an extensive use of survival analysis models, for example Kaplan-Meir curves and Cox regressions. These models have many advantages but also some statistical shortcomings such as violating at least one of the following three common significant conditions as: i) heterogeneity across individuals, ii) dependence across the number of events, and iii) both (i) and (ii). We model the prediction of survival of few thousands of CHF patients using shared frailty models (Therneau et al., 2003), that overcome the shortcomings of the Cox Models. It chains a random effect to incorporate unobserved heterogeneity with event-based stratification (varying baseline hazards) to incorporate event dependence. The event modeled here is the patient mortality. The sample is from the Sheba Medical Center patients with CHF as the primary diagnosis. Modeling and applying the shared frailty model (that includes random effects, which are taken into account on the hazard function) provides enhanced scores as compared to the traditional Cox regressions. In the next steps, we intend to elaborate the model by including additional constraints.

Keywords: Congestive heart failure, machine learning, shared frailty models, Cox model.

References:

Therneau, T. M., Grambsch, P. M., & Pankratz, V. S. (2003). Penalized survival models and frailty. *Journal of computational and Graphical Statistics, 12*(1), 156-175.

Wang, Y., & Byrd, T. A. (2017). Business analytics-enabled decision-making effectiveness through knowledge absorptive capacity in health care. *Journal of Knowledge Management, 21*(3), 517-539.

International Institute for Applied Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

Social*NAO* – A personalized learning workshop for elderly guided by a humanoid robot

[Research-in-Progress]

Dan Kohen-Vacs, Holon Institute of Technology (HIT), Israel, mrkohen@hit.ac.il

Gila Kurtz, Holon Institute of Technology (HIT), Israel, gilaku@hit.ac.il

Extended Abstract

Humanoid Robotics (HR) is an emerging field striving to deploy devices capable of resembling and mimicking human form, movement, gestures, and behaviors. For the past two decades, researchers and practitioners focus their effort as they intend to evolve robot's capabilities to interact with humans (HRI). This field has proved to be contributory in various areas, including in education for early childhood and as supportive means offered for children with disabilities. Additionally, HR was implemented in scenarios concerning care services offered for elderly (Beuscher et al., 2017; Moro et al., 2019). However, robots' implementation in light of learning processes focused on elder populations is rare. In this study, we outline the design and experiment of a personalized one-on-one workshop for seniors on the topic: social network - Instagram facilitated by NAO - a humanoid robot. As a workshop facilitator, NAO asked questions, provided ongoing feedback, and offered progress tracks desired by the learner (see a clip here). The workshop was recorded on video for evaluation practiced by ten elderly interviewees. They were interviewed on their overall assessment of the activity and its effectiveness and readiness to participate in this type of personalized workshop guided by NAO. The results were very encouraging on the feasibility that NAO can serve as a tutor for elderlies in a personalized workshop. NAO's used as an instructor enhances the learners' curiosity and motivation as he fosters a creative and friendly atmosphere. This project is the second in a series of integrating human robots as facilitators in learning processes. In a previous project, we outlined the design and experiment of an escape room training activity facilitated by NAO (Kurtz & Kohen-Vacs, 2019). In both projects, learners and evaluators expressed their enthusiasm concerning their experiences involving HRI implemented in realistic settings. Both studies mark the first step towards a template for developing innovative learning and training activities supported by a humanoid robot.

Keywords: Humanoid robot, NAO, seniors, personalized learning, social network.

References:

Beuscher, L. M., Fan, J., Sarkar, N., Dietrich, M. S., Newhouse, P. A., Miller, K. F., Lorraine, C., & Mion, L. C. (2017). Socially assistive robots measuring older adults' perceptions. *Journal of Gerontological Nursing, 43*(12), 35-43

Kurtz, G., & Kohen-Vacs (2020). A team-based training game guided by a humanoid robot [Extended Abstract]. *Proceedings of the KM Conference 2020*, Lisbon, Portugal.

Moro, C., Lin, S., Nejat, G., & Mihailidis, A. (2019). Social robots and seniors: A comparative study on the influence of dynamic social features on human–robot interaction. *International Journal of Social Robotics, 11*, 5–24.

A big data visualization and analytics examination of historic data breach incidents: Uncovered cybersecurity trends

[Complete Research]

Emily Africk, USA, eafrick@umich.edu

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

Extended Abstract

Cybersecurity breaches have been growing by the day and their impacts worldwide are staggering (Privacy Rights Clearinghouse, 2019). According to a joint report between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), cyber-attacks and data breach incidents are significantly on the rise including Advanced Persistent Threat (APT), which “historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, Structured Query Language (SQL) injection attacks, spearphishing campaigns, website defacements, and disinformation campaigns” (Federal Bureau of Investigation, 2021). Additionally, data breaches have a major negative impact to organizations. This paper focuses on combining data analytics, visualization, and quantitative analyses for business intelligence in the context of cybersecurity big-data over a period of 15-years in an effort to help provide some trends from such a large dataset. A large data set containing 9,015 data breaches was provided via the Privacy Rights Clearinghouse (2019) data breach database from the start of 2005 to end of 2019. The aim of this work was to slice the data as well as represent it into a business-related visualization that may be used in the future to help executives understand complex cybersecurity breaches, their impact, and their trend over time. We have created visualization figures along with explanations of what each visualization means in the context of cyber-attacks over time. This paper was set to serve as a breakdown of the important findings from the Privacy Rights Clearinghouse data breach database of over 15-years (2019). These findings are communicated through both key numbers and quantitative analyses for business intelligence. While our paper does not cover every aspect of the dataset (due to its significant size), it serves more as a focus on two particular parts of the dataset: incident types and their volume over the 15-year timeframe to hopefully in the future help business executives visualize cybersecurity trends. This paper ends with a conclusion and discussion on how such cybersecurity visualizations can help industries along with several future research opportunities resulting from this work.

Keywords: Cybersecurity data analytics, data breach incidents, visualizations of data breaches, cybersecurity big data, data breach analytics.

References:

Federal Bureau of Investigation (FBI) (2021, April 2). *APT actors exploit vulnerabilities to gain initial access for future attacks.* https://www.ic3.gov/Media/News/2021/210402.pdf

Privacy Rights Clearinghouse (2019). *Data breach database.* https://www.privacyrights.org/data-breaches

Security breach? Do I care enough to share information? The motives, intentions, and predictors for information sharing

[Research-in-Progress]

Angel L. Hueca, CERT, SEI, Carnegie Mellon University, USA, alhueca@cert.org

Zulma V. Westney, Nova Southeastern University, USA, zvwestney@outlook.com

Kembley Lingelbach, Middle Georgia State University, USA, Kembley.lingelbach@mga.edu

Extended Abstract

In the cybersecurity domain, information sharing is an activity where individuals exchange information relevant to a current incident or can be used to prevent future incidents. However, despite the technological advances, regulations, and innovation potential, individuals still seem reluctant to share information. Information sharing includes identifying system vulnerabilities, early warnings, phishing attempts, malware, data breaches, other indicators of compromise, and general best practices. Currently, many attack detection tasks are performed within individual organizations, with little cross sector, or cross industry information sharing. The main goal of information sharing is to bring a high-level of awareness of the cyber threat landscape of a specific industry or sector, which is essential in effective preparation in overall cybersecurity incident response.

An organization's ability to respond to information security incidents is influenced by the group of employees within a department, and the overall culture of the organization. The diversity and the multigenerational composition of an organization's workforce pose a significant challenge for cybersecurity leaders considering today’s increasingly competitive environment. Previous literature indicates that people belonging to the same generation share similar historical, social, and cultural attitudes and values. Business research literature highlights that each generational group has different values and characteristics that directly impact attitudes and behaviors at work. This study will examine the demographic and generational differences in sharing security information by valuing the sources of motivation, intentions, and trust between millennials and older generations to assist cybersecurity professionals in making information-sharing decisions. For example, Twenge et al. (2010) indicated that some employee groups are more capable than others in recognizing, responding, and sharing information about security incidents in a manner that is consistent with the organization's collective security protocols.

Keywords: Information sharing, generational studies, cybersecurity, millennials, demographics.

Reference:

Twenge, J. M., Campbell, S. M., Hoffman, B. J., & Lance, C. E. (2010). Generational differences in work values: Leisure and extrinsic values increasing, social and intrinsic values decreasing. *Journal of Management*, *36*(5), 1117–1142.

What impact does gamification have on cybersecurity student engagement and satisfaction during the COVID-19 pandemic?

[Research-in-Progress]

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

Gerald Emerick, Ferris State University, USA, jerryemerick@ferris.edu

Greg Gogolin, Ferris State University, USA, greggogolin@ferris.edu

Extended Abstract

In this study, Capture The Flag (CTF) gamification of cybersecurity concepts were delivered virtually to students during the COVID-19 pandemic. During this time, cybersecurity classes were held 50% virtually via Zoom, and student class participation and interaction is decreasing at an American university in the Midwest. In order to increase student engagement, excitement, and skills development of cybersecurity concepts, three CTF competitions will be delivered to students during school semesters in 2021 online using Zoom. One CTF will be delivered to university students enrolled in a cybersecurity degree. Two CTFs will be delivered to STEM students enrolled in midwest high schools in the United States. All students were between the ages of 16-21. Surveys will be developed to students both before and after the CTF to measure interest in cybersecurity, excitement towards online learning, interest towards online gamification, effectiveness of CTF delivery of cybersecurity concepts and questions, and student motivation to participate in online activities during the COVID-19 pandemic. This study will help faculty understand and evaluate the effectiveness of engaging, gamified delivery of cybersecurity concepts, as well as develop a framework for engaging online activities to increase student engagement, excitement, and skills development of cybersecurity concepts. A current gap in the examples of gamification strategies to motivate students in a pandemic setting is an opportunity to measure effectiveness of online gamification. Results from the engagement surveys will be utilized to determine the effectiveness of cybersecurity gamification, virtual competition interest, and overall interest in cybersecurity despite pandemic circumstances.

Keywords: Gamification, cybersecurity, CTF, virtual learning, student engagement, skills development, pandemic.

Knowledge sharing best practices in management consultancy-driven culture

[Practitioner's Presentation]

Evgeniya Ivanova, CORE SE, Germany, evgeniya.ivanova@core.se

Extended Abstract

Today still a lot of companies are daily confronted with the weak knowledge management and unsuccessful or incorrectly applied knowledge sharing mechanisms and methodologies. Even more, some management consultancies have lack of awareness and knowledge of what are the modern and successful knowledge sharing mechanisms in the organizations as well as what are their strategic business outcomes and effects today. We propose to present the applied knowledge sharing mechanism based on internal corporate culture as it is significant for the management consultancies to achieve success and strategic goals. It systematically secures the experience, expertise, tacit and explicit knowledge of employees and company, helps to acquire new projects faster, to expand the company's core competences, to develop new competences and to strengthen market position and industry competitiveness. The relevance of the proposed topic is confirmed by the finding that corporate culture and the exponentially developing technologies nowadays determine the mechanism of knowledge sharing in the companies, since they have a direct impact on learning and knowledge sharing behavior of employees. Focus will be on the internal analysis of the organizational pillars to identify the weaknesses and knowledge management barriers in the company, implement the proposed mechanism of knowledge sharing to cover it, create an environment to share creative ideas, generate new knowledge, keep track innovations, and market related know-how, lessons learned as well as acquire, codify, and share most related knowledge and transfer it among the company. We believe that establishing the proposed knowledge sharing best practices, creation and promotion of knowledge sharing culture by exchanged and coordinated information resources and knowledge communities as well as platforms to improve access to knowledge and information repositories through modern technologies will lead to the company's transformation in a learning organization in which knowledge plays a crucial role in achieving strategic goals.

Keywords: Knowledge management, knowledge sharing, knowledge sharing best practices in management consultancies, management consultancies.

Academic and practitioner perceptions of salient knowledge-related risks

[Research-in-Progress]

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

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

Extended Abstract

Risk assessment in information systems typically focuses on Information Technology (IT) project risks (Alarabiat & Ramos, 2019), which is not surprising, considering the frequency of project failure. Research interest in the ongoing management of knowledge-related risk as part of organizational risk management is relatively neglected and under-theorized (Durst, 2019). Whilst knowledge management scholars recognize a multitude of potential threats, risk management practitioners have to manage knowledge-related threats in parallel with others that are perceived to be more concrete. Furthermore, the possible knowledge-related risks are numerous and there is no definitive list of the most salient risks.

The research identifies salient knowledge-related risks in organizations by conducting a ranking-type Delphi study with two panels of experts: academics and practitioners. The academics were selected from the fields of knowledge management and cybersecurity. Whereas the practitioners from knowledge management and risk management departments in business firms. The panels of experts were presented with an initial list of knowledge-related threats derived from the literature and asked to rate the risk of each threat on a Likert-scale with the goal of paring down the list to a maximum of 22 items. During further rounds the panels were asked to choose the threats posing the biggest and the smallest risk from sets of items drawn from the pared down list. As part of the second round, the experts could explain their choices in comment blocks and these comments are visible to peer respondents in the following rounds until sufficient consensus is reached on the ranking. Finally, the resultant ranking of salient risks are presented and the perspectives of the academic and practitioner panels compared. In conclusion, the plausibility of reconciling the differences between groups is discussed.

Keywords: Knowledge management, knowledge risk assessment, risk management.

References:

Alarabiat, A., & Ramos, I. (2019). The Delphi method in information systems research (2004-2017). *The Electronic Journal of Business Research Methods, 17*(2), 86-99. https://doi.org/10.34190/JBRM.17.2.04

Durst, S. (2019). How far have we come with the study of knowledge risks? *VINE Journal of Information and Knowledge Management Systems*, *49*(1), 21–34. https://doi.org/10.1108/VJIKMS-10-2018-0087

Cyberslacking during COVID-19 pandemic: The experience of students in a virtual environment

[Research-in-Progress]

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

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

Extended Abstract

The impact of the COVID-19 pandemic in 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 were encountering 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 define as the time that students spend for 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 SMS messages (Gerow et al., 2010; Simanjuntak et al., 2019). It is possibly that this kind of behavior increased during the COVID-19 pandemic, because 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 professor are limited. This study will examine the cyberslacking behavior of these students during COVID-19 pandemic and their academic success during this time. Also, the study will compare the academic success differences between those that admit their cyberslacking behavior versus those that were not doing it. The study will use an anonymous survey as a methodology that includes cyberslacking activities and their academic success during that academic year. The study will contribute to the expansion of cyberslacking knowledge base in the academic environment and to develop new cyberslacking studies in universities after COVID-19 pandemic. 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.

References:

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.

Simanjuntak, E., Fardana Nawangsari, N. A., & 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. https://doi.org/10.3390/bs9120123

International Institute for Applied
Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

COVID-19 effect on the healthcare sector's cybersecurity

[Complete Research]

Ruti Gafni, The Academic College of Tel-Aviv Yaffo, Israel, rutigafn@mta.ac.il

Tal Pavel, The Academic College of Tel-Aviv Yaffo, Israel, talpv@mta.ac.il

Extended Abstract

This research aimed to reveal whether the COVID-19 pandemic was a trigger to cyberattacks targeted to the healthcare sector. The research aim was to determine in which manner the COVID-19 pandemic affected the number and essence of cyberattacks reported during the year 2020 in the healthcare sector, in comparison to the parallel period prior to the pandemic. The study was based on published items in two main websites, which review such incidents, and were found to be the richest, with a big gap from all other websites: www.beckershospitalreview.com and www.healthitsecurity.com. The items were collected from both websites from 1 January 2019 until 31 December 2020.

The total number of published reports on cybersecurity against the healthcare sector during 2019 and 2020 was 1,397, where Becker's Hospital Review published 1,000 items, and Health IT Security reported 397. The reports were examined in order to choose those regarding specifically to cyberattacks to the healthcare sector, leaving 764 reports to analyze, 327 in 2019 and 437 in 2020, consisting an increase of 34 percent in reports on cyberattacks in the healthcare sector. It is important to clarify that the COVID-19 emerged in December 2019, in which 40 relevant reports were found. The number of cyberattacks fits interestingly the pattern of waves of the pandemic, which expanded worldwide, with a most outstanding increase in the first months after the outbreak, in December 2019, and January 2020. During the first wave of the pandemic, the number of reports was doubled or even tripled, compared to the same period in 2019, a tendency that was slightly waned afterwards. A parallel comparison of the monthly attacks, 2019 against 2020, shows a higher number of reports almost for each month. The increase in the volume of cyberattacks was felt mostly in the first quarter of 2020, whereas after was a slight decrease which can be explained by four different factors: (1) the attack goal, (2) the attacked factor, (3) the attacker factor, and (4) the level of awareness and protection. In addition to cybersecurity attacks on the healthcare system, the COVID-19 pandemic created long-term wide-range changes that affect every individual and sector, mainly due to the shift to a remote working model, which imposes long-term new cybersecurity changes, among them to the healthcare industry.

Keywords: Cybersecurity, coronavirus, COVID-19, healthcare, cyberattack.

Autonomous educational software for learning Hebrew with gamification and crowdsourcing

[Research-in-Progress]

Rina Zviel Girshin, Ruppin Academic Center, Israel, rinazg@ruppin.ac.il

Nathan Rosenberg, Paralex Research, Israel, paralex.research@gmail.com

Extended Abstract

In recent years blending of education and entertainment created a new industry called edutainment (Aksakal, 2015). Game-Based Learning (GBL) is on the rise, especially now with all COVID-19 disruption of education. In this study, a gamified crowdsourcing autonomous software system for learning how to read in Hebrew is presented. The system uses crowdsourcing approach for resource gathering. The main goal of the system is to help children to acquire basics reading skills. The design of the system is done according to Keep It Simple principles and a responsive design approach. The system has three types of users: a guest learner, an identified user and a crowd (parent/teacher). The software has three major modes: training; playing and testing; reports, and crowd data gathering. Crowdsourcing is a technique of gathering data or performing large scale tasks by outsourcing it to a wider public. Its role and potential in language education is investigated in enetCollect (EU Network for the Combination of Language Learning and Crowdsourcing Techniques) COST action. The current software was designed as a part of enetCollect research (Zviel Girshin & Raskin, 2019). The designed software is built as an autonomous system that uses crowdsourcing approach for collecting language learning educational materials. The initial system is designed by developers, but later the system grows and evolves using resources supplied and approved by the crowd. The new content is uploaded by crowd. It includes several new word related items. Later these new items are approved by group of other users. Only 100% approved content enters a database of words, which is used in future training and GBL. The designed educational software was tested for a short period of time in three kindergartens (because of COVID-19 lockdown). The data gathering approach is experimented and evaluated in comparison to traditional data preparation techniques in the field of language learning. The researchers made a detailed analysis of the collected data set to evaluate the success of the proposed approach. The researchers monitored the child's involvement (number of games played, correct incorrect answers, average time for play), system usage (average time for play, daily, weekly entrances to the system) and parents' willingness to contribute and approve new content.

Keywords: Crowdsourcing, edutainment, gamification, educational software.

References:

Aksakal, N. (2015). Theoretical view to the approach of the edutainment. *Procedia-Social and Behavioral Sciences*, *186*, 1232-1239.

Zviel Girshin, R., & Raskin, A. (2019). Educational software for learning Hebrew with gamification and crowdsourcing. *Proceedings of the COST EnetCollect WG3/WG4*.

Knowledge management tools, methods, and models in the context of SMART governments: A literature review

[Research-in-Progress]

Ashraf Munib Ahmed Qutaishat, University of Minho, Portugal, qash99@yahoo.com

Isabel Ramos, University of Minho, Portugal, iramos@dsi.uminho.pt

Extended Abstract

The high volume of available data and the continuously increasing gap between what governments know and what they do with it can either promote or hinder government decisions and the quality of their attention. However, the rise of smart cities and the aim to enable societies to prosper have persuaded governments to transform their services into smart services and transform themselves into smart governments by benefiting from the integration and intelligent use of innovative technologies, including social media technologies to support Management By Objectives (MBO) and set Specific, Measurable, Achievable, Realistic, and Time-based (SMART) goals through a transparent and inclusive citizen collaboration (Qutaishat & Alex, 2018). Thus, our research question is: "What is the state-of-art of research into knowledge management tools, methods, and models within the smart government context?" The paper aims to explore state-of-the-art research in knowledge management within the smart government context from 2018 to 2020 and contributes to aiding researchers in mapping the field to identify which themes they should invest their time and efforts investigating. We have sampled 301 publications, then utilized a systematic literature review combined with a mixed-method of analysis to analyze the sample according to defined criteria. This has resulted in our final repository so far containing 40 Scopus indexed papers. The repository distribution was as follows: 48% from 2018, 43% from 2019, and 10% from 2020. Moreover, 10% were from conferences and 90% from journals. Preliminarily, we found 38% of publications focused on the effects and implications of KM on smart governments in 2018 compared to 67% in 2019 and (3) publications in 2020. Furthermore, 31% focused on knowledge sharing and transfer in 2018 compared to 19% in 2019 and (1) publication in 2020. We also found that 34% used case studies and 28% utilized surveys, while 22% focused on literature reviews and 16% on interviews.

Keywords: Knowledge management, smart government, social media monitoring, systematic literature review, mixed-method of analysis.

Acknowledgement:

This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Units Project Scope: UIDB/00319/2020.

References:

Qutaishat, A. M. A., & Alex, K. (2018). Open innovation for smart government: A literature review. *Proceedings of the CAPSI 2018*, Portugal. https://aisel.aisnet.org/capsi2018/27

Relationships between foresight and knowledge management processes from the perspective of the theory of creation of organizational knowledge

[Complete Research]

Alan Rafael Boesing, Universidade Federal do Rio Grande do Sul, Brazil, aboesing@hotmail.com

Raquel Janissek-Muniz, Universidade Federal do Rio Grande do Sul, Brazil, rjmuniz@ufrgs.br

Extended Abstract

Foresight deals with the organization's ability to anticipate external changes and incorporate information in its strategic formulation, which is important to ensure its survival and growth. Moreover, being able to make the selection, interpretation and integration, so that a set of useful and applicable knowledge is created, would be the real advantage of an organization. This paper is justified by the proposition that both the development and the result of the foresight, based on its characteristics can leverage knowledge management to provide effectively oriented actions and practices for the future. The importance to Knowledge Management (KM) is due to the use of a hitherto unprecedented approach on the subject, using quantitative and qualitative methodology for the exploration of the subject, in an attempt to narrow the gap between foresight and KM practices. The first Research Question (RQ1) asks "Is there a significant relationship between foresight and the processes of knowledge acquisition, conversion and application?". RQ1 was answered in the affirmative, using the statistical method of Partial Least Squares (PLS) regression with 30 online surveys with specialists. The hypotheses that relate the foresight to the acquisition, conversion and application of knowledge were supported by the t-test, presenting a moderate Pearson determination coefficient (R^2) and positive predictive quality. RQ2 asks "The foresight process is responsible for what types of knowledge conversion according to the SECI model?", and RQ3 asks "How can the conversions that occur during foresight be represented?" Both were answered using seven interviews with foresight specialists. It was found that the foresight process is responsible for all types of knowledge conversion in the Socialization, Externalization, Combination, and Internalization (SECI) model, but with different intensities. Theoretical implications of this work are the confirmation of the relationship between foresight and knowledge management and the proposal of a model that encompasses this relationship. In the practical field, the indication of the approximation of the areas of foresight and knowledge management is one of the contributions of the study. Another contribution is the need for valuing tacit knowledge in the figure of foresight specialists, constituting an intangible asset of the organization and which should be encouraged by managers and senior management. The practice of promoting the socialization of top management as foresight specialists is another finding of this article, in order to contribute or change the knowledge framework of those responsible for the organization's strategic decisions.

Keywords: Foresight, knowledge management, mixed methods, SECI model.

International Institute for Applied Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

The paradox of personalized and adaptive learning

[Research-in-Progress]

Amir Winer, The Open University of Israel, Israel, amirwi@openu.ac.il

Nitza Geri, The Open University of Israel, Israel, Nitzage@openu.ac.il

Extended Abstract

From the very beginning of our life we find ourselves as members of communities. The manifestation of communities within Virtual Learning Environments (VLEs) is mostly associated with the connectivist approach in which learning occurs when knowledge is actuated by learners connecting to and participating in a learning community. Learning communities are "the clustering of similar areas of interest that allows for interaction, sharing, dialoguing and thinking together" (Siemens, 2005). In a seemingly counterintuitive move, learners become accustomed to being constantly connected through the VLEs and together with others, yet they feel more alone in comparison with face-to-face learning. This phenomenon has been identified by Turkle (2011) as the 'alone-together paradox'. We suggest that this paradox is amplified by VLEs that promote personalized and adaptive learning designs. Personalization provides learners with a multiplicity of parallel options for learning and the freedom to select among them. Adaptive learning allows smart capabilities that cater a unique learning experience for each digital learner based on their actual learning progress. Whereas the connectivist approach was originally designed to support a network model (many-to-many) for learning communities, personalized learning is mostly associated with a star-like (one-to-many) community model. Within this context, the purpose of this study is to develop design principles for VLEs in higher education that will aim to strengthen the sense of community in VLEs. Our research follows the three cycle view of the design science research paradigm: Relevance, design, and rigor (Hevner, 2007). We focus on the critical challenge of shifting the role of learning analytics tools from the personalized measurement of digital learners to performance measurements that consider digital learners as community members. We provide some initial VLE design insights that might support the establishment, nurturing, and the continuing presence of virtual communities for digital learners.

Keywords: Personalized learning, sense of community, learning communities, learning design, learning analytics.

References:

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems, 19*(2), 87-92.

Siemens, G. (2005). Connectivism: A learning theory for the digital age. *International Journal of Instructional Technology and Distance Learning*, *2*(1).

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

Virtual hybrid design for learning humanistic management

[Research-in-Progress]

Julita Haber, Fordham University, USA, jhaber7@fordham.edu

Sophia Town, Fordham University, USA, stown@fordham.edu

Christine Janssen, Fordham University, USA, cjanssen@fordham.edu

James Teague, Fordham University, USA, jteague@fordham.edu

Extended Abstract

Amid many online teaching initiatives during the COVID pandemic, we managed to build a unique virtual platform for a Principles of Management course that attracted attention from other universities around the globe. Infusing a top-of-the-line learning system with groundbreaking humanistic management content, we developed an innovative and engaging experience for future leaders, in lieu of a traditional textbook. TalentLMS is a cloud-based learning management system for midsize businesses and one of the best-rated training systems today.

The newly revised course was set up to prepare students for the 21st Century business environment by focusing on a truly humanistic approach to management and leadership. A team of the management faculty area developed own curated videos, audio clips, texts, and added sources from other experts. We integrated mindfulness, meditation exercises, social innovation and sustainability to pioneer an approach of *knowing*, *doing*, and *being* in business. The course was modular in nature. Six hundred students progressed through TalentLMS by responding to questions and reflecting on the material between sections to deepen their knowledge and retention. The online format allowed for a flipped course format where students completed the online material on their own time (asynchronously) and then met live with faculty either online or face-to-face in a classroom (synchronously).

We measured the effectiveness of our efforts with a number of feedback surveys (mid-term and post-term). The post-term survey resulted in 170 responses and a 35% response rate, indicating increased student engagement where 73% liked the TalentLMS platform, 60% enjoyed the self-paced format and flexibility, and 58% students rated the system as user friendly. Written reflections at the end of each module confirmed students' deeper understanding and internalization of course concepts. Although we instituted end-of-module quizzes, it was challenging to objectively assess the actual learning from the revised course. We required students to spend three hours in completing the asynchronous content without considering adverse effects of students' screen time; this proved to go against our teaching of humanistic concern for people's well-being. Moving forward, we are revising the course for more short sound bites of information, summaries, streamlining the content, and improving assessment techniques.

Keywords: Management knowledge, humanistic management, learning system, mindfulness, meditation, online learning.

International Institute for Applied
Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany
A Publication of the International Institute for Applied Knowledge Management

A review of industry experts' perceptions of knowledge security

[Complete Research]

Christopher Shear, Department of Information Science, Stellenbosch University, cj52za@yahoo.com

Bruce Watson, School for Data-Science & Computational Thinking, Stellenbosch University, bruce@bruce-watson.com

Martin Van der Walt, Centre for AI Research (CAIR), Stellenbosch University, msvdw@sun.ac.za

Extended Abstract

The review forms part of the paper focused on the development of a conceptual model of knowledge security, where the insights derived will be used as inputs for the development of the model. As part of the practical research component, a series of interviews were conducted with industry experts. This was done to better understand the role of Knowledge Management (KM) and its relationship with security in organizations; by illuminating any associated issues in context. The research is premised on the view that for today's organizations, knowledge has become a highly valuable resource that is often critical for competitive success. As organizational knowledge has value, for both the organization and other external entities too, it needs to be protected. In response, the idea of knowledge security has emerged as a mechanism to protect organizational knowledge. But how it is perceived in practice, and its broader relationship with KM, is not always clear. This poses a risk for organizations, due to the increasing complexity of the intelligence gathering mechanisms used by malicious entities, and the need for organizations to ensure the internal viability of this resource. Examining how KM and security are perceived practically, should be of interest to conference participants wanting to deepen their understanding of this topic. The review followed an interpretivist paradigm centered on a qualitative case-based research methodology, using a case-based analysis approach for data collection. An expert centered approach was taken, with the unit of analysis focusing on interviewing experienced industry experts. A sample size of between 5-10 experts was deemed appropriate to fulfil the objectives of the research, with nine experts having participated in the final study. The participants had an average of 24 years of experience with all having some knowledge of KM and/or security. The process of analysis and interpretation took place through five phases consisting of the interviews, transcription and capturing notes, case study narratives, cross-case analysis and interpreting and enfolding the findings. The findings from the interviews showed that knowledge security is often orientated towards the tangible aspects of KM, with the nuanced aspects not always considered. The broader implication of this is that the knowledge security measures put in place are not always as effective as they could be. This can result in the possibility of unidentified knowledge risks emerging and therefore affecting the long-term security of an organization's knowledge.

Keywords: Knowledge management, information security, risk management.

International Institute for Applied Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany

A Publication of the International Institute for Applied Knowledge Management

Exploratory and real-time data science on MITRE's ATT&CK framework

[Research-in-Progress]

Liam Watson, Computer Science Department, Somerset College, South Africa, liam@ip-blox.com

Bruce W. Watson, Information Science, Centre for AI Research, School for Data-Science & Computational Thinking, Stellenbosch University, South Africa, bruce@bruce-watson.com

Extended Abstract

MITRE's ATT&CK is one of the most complete knowledge representations of cyber threats – providing not only a breakdown of the best-known threats, but also a taxonomy/ontology of the threat techniques (i.e. the specific *hacks* used by the threat). This gives insight into how the attack is structured, as well as possible defences. The ATT&CK website provides different visualizations, including a threat matrix and an online tool for exploring the threats. Furthermore, several papers have appeared using alternative visualizations and uses of the taxonomy, which is now forming the core of some tools for threat hunting and classification.

In this research, we provide an alternative representation of ATT&CK – using a *Formal Concept Lattice* (FCL). FCL's are rooted directed graphs (much like a tree, but with sharing of subtrees) which highlights the commonalities and differences between *objects* (the cyber threats in our case) with respect to their *attributes* (the hacking techniques of the threats). Specifically, the graph nodes represent sets of attributes, starting with the empty set ("no attributes") at the root, and growing downwards until all objects appear.

In addition to commonalities/differences, additional relationships of importance can be directly read from the FCL graph (unlike in most other structures): *synonyms* are shown as two attributes on the same node; *implications* are shown as upward connections; *distinguishing attributes* are those which can quickly disambiguate between two choices; and, *minimal attribute query sequences* show how to disambiguate between threat actors.

An FCL for the "mobile devices" part of ATT&CK has been built and analyzed, allowing for some specific insights: *overlaps between cyber threats* highlight which hacking techniques they have in common; *attribution signatures* are emerging – with specific clusters of techniques pointing to certain cyber threat actors; maliciously, *opportunities for hybridization* can be found by combining components in ways not yet shown in the FCL (exploring the "open" parts of the FCL graph), thereby yielding or predicting new threats; with only a few observations of techniques (hacker moves) in a system, the *likely outcomes* are visible in the FCL, allowing for pre-emptive defence to be done in *real-time*; lastly, *real-time and incremental expansion (build out)* of the FCL is possible as new threats arise, all using a variety of new algorithms.

Keywords: Data science, correlation algorithm, formal concept lattice, ATT&CK, AI, machine learning, data visualization.

A cyber-robust architecture for decision-support systems

[Research-in-Progress]

Nanette Saes, Information Science, Centre for Decision-Making and Knowledge Dynamics, Stellenbosch University, South Africa, nanette@xpattycake.com

Bruce W. Watson, Information Science, Centre for AI Research, School for Data-Science & Computational Thinking, Stellenbosch University, South Africa, bruce@bruce-watson.com

Extended Abstract

Decision-making is the single most important and sensitive "business process" in militaries, intelligence agencies, governments, and businesses. The commonly-used Data-Information-Knowledge-Wisdom (DIKW) pyramid gives structure to decision-making ingredients: *Data* is the basic low-meaning stream, which is lifted to *Information* by adding semantics, which contributes to *Knowledge* by interconnecting information insights and patterns, and finally *Wisdom* which encompasses possible actions – enabling decision-making. These levels are brought to life in many types of decision processes, e.g. the familiar Observe-Orient-Decide-Act (OODA) loop. Fast high-quality decisions are a universal aim and also a major goal of AI and data-science. Furthermore, *explainable decisions* (with an audit-trail and provenance of the inputs) are important but rarely implemented. AI-driven *Group Decision Support Systems* (GDSS) are one way to fuse qualitative and quantitative decision-making – typically with specialized software over a network, and human (for now) decision-makers/participants at their own laptop. In addition to structuring the process, GDSS enable parallelism (participants simultaneously giving decision input), distribution, and anonymity when needed.

Cybersecurity has traditionally also followed the first levels of the DIKW pyramid – primarily focusing on *data-security* (treating it as a purely technical or encryption problem), or *information-security* (as an organizational or business-process problem), with some (including our group) now also advocating for *knowledge-security*. In this research, we argue for *wisdom-security* as the required next level. Globally, COVID-19 has rapidly forced even more decision-making online and distributed – dramatically enlarging the *attack surface*. Attacks on decision-making can take many forms, most of which are very sophisticated and form *Advanced Persistent Threats*, with strategies such as: corrupt the inputs to nudge decisions; remove inputs to degrade decisions; fundamentally alter knowledge; inject a witting insider to corrupt the process; removal or delays in (parts of) the decision-making structure; and corrupt the output decision or explanation. First, we consider the fundamental building blocks of GDSS, their inputs and vulnerabilities. This is used to motivate for a new architecture that is robust against almost all of these threats (the witting insider remains difficult) by using emergent technologies: decision-input signatures, information provenance tracking and ranking, fail-functional business processes, output (and input) decision signatures, and block-chain.

Keywords: Decision-making, wisdom-security, GDSS, cyber-robust architecture, decision signatures, DIKW hierarchy, block-chain.

Supply chain cyber-attacks: Evaluating the impact of supply chain cyber-attacks on the South African public procurement legislation

[Research-in-Progress]

Given Shingange, Department of Information Science, Centre for AI Research, Stellenbosch University, given.shingange@icloud.com

Bruce Watson, Department of Information Science, Centre for AI Research, School for Data-Science & Computational Thinking, Stellenbosch University, bruce@bruce-watson.com

Extended Abstract

The research investigates the suitability of the South African Procurement laws in preventing *supply chain cyber-attacks*. The recent *SolarWinds* attacks have brought the supply chain attacks into the spotlight (Baker, 2021). Many countries and organizations are working on ways to avoid such attacks. The SolarWinds attack involved hackers compromising the infrastructure of the company called SolarWinds. This company produces a network- and applications-monitoring platform called *Orion* and then using that access to produce and distribute "Trojanized" updates to the software's users. Due to the SARS-Cov-2 pandemic, we have had to change how we work, and the number of people working from home has increased. As a result of the government restrictions, public and private organizations have had to change how they use their current Information and Communication Technology (ICT) infrastructure. In all this, the South African government departments have had to adapt to the new context, which has led to the putting aside some of the procurement requirements as prescribed by the Public Management Finance Act, No 29, 1999 (PFMA). The PFMA will be analyzed to determine if it is easier for supply chain cyber-attacks to be carried out. South Africa's power utility, Eskom, is used as a case study to determine if the organization does not expose itself to possible attacks in the recent procurement of ICT support services (Ellis & Levy, 2009). The primary implication of the study is that it will set the groundwork for the reviewing of procurement laws to suit the current cyber threat environment. This should help organizations and government departments to improve their procurement processes while staying secure. A supply chain leapfrogging framework will be developed as a basis for adapting the laws accordingly.

Keywords: Supply chain cyber-attacks, leapfrogging, SARS-Cov-2.

References:

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology, 6*, 323-337. https://iisit.org/Vol6/IISITv6p323-337Ellis663.pdf

Baker, P. (2021). The SolarWinds hack timeline: Who knew what, and when? *CSO*. https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html

International Institute for Applied
Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany
A Publication of the International Institute for Applied Knowledge Management

Working from home, not working insecurely

[Research-in-Progress]

Neal Kushwaha, IMPENDO Inc., Ottawa, Canada, neal@impendo.com

Bruce Watson, Info Science, Centre for AI Research, School for Data-Science & Computational Thinking, Stellenbosch University, bw@bruce-watson.com

Extended Abstract

Under the coronavirus pandemic, governments and corporations around the world have adopted a *Work-From-Home* (WFH) mode of operations to continue governing and operating. Over a year later, many continue to WFH and a large majority have little plans to return to an office building. Early on, governments and companies scrambled to increase Virtual Private Network (VPN) licenses and bandwidth capacities to take on the additional user load at a technical level. This allowed a near seamless continuance of communications for common unclassified information and other designate information (non-national interest) with authorised software encryption. But what about the classified information (national interest)?

Within weeks, government departments began discussing deploying classified access from home, and later in the summer of 2020, some deployed the offering, including US Army Army Network Enterprise Technology Command (NETCOM) deploying access to Secret Internet Protocol Router Network (SIPRNet) for over 2000 users. While policies and legal constructs exist to ensure classified material remain in controlled facilities, some departments have accepted the risks so that they may continue to govern. This abstract serves as an outline to discuss the impacts (to the individual and government) while accessing, consuming, and created classified content from home in six (6) security domains and two (2) major threats to classified information.

The six areas of security include (1) Operational Security (OPSEC) policies, (2) Physical Security (PhySec) policies, (3) Communication Security (COMSEC) doctrine, (4) Information Technology Security (ITSEC), (5) Personnel Security (PERSEC) policies, and (6) Emanations Security (EMSEC) concerns. When considering security of technological systems, focus tends to be on encryption (including data at rest and in transit) and credential safeguarding. In practise and for classified systems, there is much more to consider, especially under when working from home.

Further, our study will focus on two major threats to classified information, specifically (1) insider threats and (2) foreign state actors (located both domestically and abroad) when working from home versus in an authorised government facility. The entire study will investigate the risks governments have accepted to support classified WFH under the pandemic with the intention to help governments better understand the risks they accepted and how their decisions may impact their operations and state security in the near to longer term.

Keywords: Work-from-home, security policies, government, foreign state actors.

Developing problem solving skills in data structure course: The case of information systems students

[Complete Research]

Sofia Sherman, The Academic College of Tel Aviv–Yaffo, Israel, shermans@mta.ac.il

Orly Barzilai, The Academic College of Tel Aviv–Yaffo, Israel, orlyba@mta.ac.il

Moshe Leiba, The Academic College of Tel Aviv–Yaffo, Israel, mosheli@mta.ac.il

Extended Abstract

Data Structures and Algorithms (DS) is a required course in the Information Systems (IS) discipline, where students undergo a problem-solving process and develop necessary skills. During such a process, knowledge is continually created, stored and retrieved, and further used as a prerequisite for taking advanced courses of IS curricula. While the literature acknowledges this course difficulty, little reference was found to the process students undergo, when solving an algorithmic problem. Our research objective is to describe both the process followed and the cognitive attributes used by students during problem solving requiring abstract thinking.

To this end, an exploratory qualitative case study was conducted within the DS course for IS students. During the study, thirteen students, solving a complex problem were observed, using think aloud techniques. Each observation was recorded, transcribed, and iteratively analyzed using principles of provisional coding in qualitative data analysis. A problem-solving steps framework, defined for programming processes, proposed by Cakiroglu and Mumcu (2020) and cognitive attributes effecting this process based on the cognitive attributes described by Leiba (2010) for mathematical problem solving were used.

Findings suggest that the quality and correctness of the solutions depend on: (1) Problem-solving process including problem understanding, solution and summary; (2) Different order of these steps (iterative vs. linear); (3) Cognitive aspects related to different levels of abstraction thinking and misconceptions during these steps; and (4) Tools student use as scaffolding, e.g., visualization of the different steps of the solution, writing a pseudo code and data sets' simulation. The study results will improve the IS community understanding of the problem-solving process experience, its attributes and the knowledge needed when confronted with complex algorithmic problems.

Keywords: Data structure course, information systems undergraduates, problem solving process, cognitive attributes, complex algorithmic problems, abstraction thinking, qualitative study.

References:

Çakıroğlu, Ü., & Mumcu, S. (2020). Focus-fight-finalize (3F): problem-solving steps extracted from behavioral patterns in block based programming. *Journal of Educational Computing Research, 58*(7), 1279-1310.

Leiba, M. (2010). Assessing mathematical problem-solving behavior in web-based environments using data mining. In *EC-TEL Doctoral Consortium* (pp. 37-42).

International Institute for Applied
Knowledge Management

Refereed Extended Abstract Proceedings - KM Conference 2021 – Leipzig, Germany
A Publication of the International Institute for Applied Knowledge Management

Exploring career path strategies for women in IT managerial positions: US and Polish perspectives

[Research-in-Progress]

Michelle Ramim, Dr. Kiran C. Patel College of Osteopathic Medicine, Nova Southeastern University, USA, ramim@nova.edu

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

Extended Abstract

Workforce diversity in Information Technology (IT) professional careers has been long recognized as desirable. IT job roles appear to be increasingly attractive for women over the past decade, consequently, women around the world have attained higher education degrees and acquired IT jobs at an extraordinary pace. Yet the Global Gender Gap Index indicated that gender gaps in IT managerial roles remained staggered (World Economic Forum, 2021). Women representation has narrowly improved overall in IT professional positions, though certain positions such as data scientist, artificial intelligence engineer, and cloud engineer women' share is in the single digit percentage of the workforce. This is mainly attributed to the lack of technical knowledge, skills, and proper relevant academic degrees. This study explores the following Research Questions (RQs): RQ1: What are the academic and professional backgrounds of women in IT managerial positions? RQ2: What career strategies did women follow to obtain IT managerial positions? RQ3: Are there significant mean differences in women' career path strategies between United States (US) and Poland? The focus is on women in US and Poland, exploring their career path strategies in IT managerial positions including motivation, background, knowledge/skills, and strategies to advance in the field. The sample includes 25 in-depth semi-structure interviews with US women working in healthcare IT managerial positions and Polish women working in IT managerial positions in banking and telecommunication sector. Initial results indicates that, surprisingly, majority of the interviewees did not study IT, rather graduated from business or nursing in the US, or economics with finance and banking specializations in Poland. The women in the sample followed three different strategies to succeed: (1) hard working, ability to gain technical skills on the job, and demonstrating high performance over years in the industry; (2) ability to be assertive and demonstrating self-confidence when making decisive decision and standing behind their decision with strong facts' (3) working with a mentor who can guide their personal vision on how to advance in their career path and improve themselves. Many women are successful in IT managerial career path, increasingly having an IT degree, enhances their performance with less learning as they go given their technical knowledge/skills.

Keywords: Women as IT managers, career strategies for women in IT, women in healthcare IT.

References:

World Economic Forum (2021). *Global gender gap report 2021*. http://www3.weforum.org/docs/WEF_GGGR_2021.pdf