IEOM
IEOM Society
International Journal of
Industrial Engineering and Operations Management
(IJIEOM)

Special Issue on

Cybersecurity in the Era of the COVID 19: A Developing Country Perspective

The International Journal of Industrial Engineering and Operations Management (IJIEOM) seeks submissions for a special issue on “**Cybersecurity in the era of the COVID-19: A developing country perspective”**.

The COVID-19 pandemic has accelerated and broadened the use of Information & Communication Technologies (ICTs) by both practitioners and academics. Many businesses, schools and universities in developing countries have, for the first time, resorted to working from home during the lockdown in compliance with national and local COVID-19 regulations, dubbed as ‘the new normal’.

Against this background of increased online activity and the ever-growing cyber threats, many organisations and individuals have become victims of cybercrime after being caught unprepared to securely conduct business online. To address the security challenges posed by the new normal, industry and academic players need to develop measures that empower society (employees, partners, contractors and learners) to work remotely without compromising security or convenience. There is an urgent need to equip a telecommuting workforce, e-learners, e-educators and online socialites. This challenge is exacerbated by the need to secure a multi-faceted terrain characterised by bring-your-own-device policies as well as blended cloud and on-premises environments.

This special issue of the IJIEOM invites full papers that examine Cybersecurity in the era of the COVID-19 pandemic from a perspective of the developing world. The objective of this special issue is, therefore, to invite academics and practitioners to contribute to a better understanding of Cybersecurity within the context of the COVID-19 pandemic and developing nations. In this context, Cybersecurity real-world applications and business models, including company case studies dealing with Cybersecurity, theoretical papers, review papers and methodological papers may provide better guidance for companies and society, in general, to protect themselves against cybercrime. In particular, this includes practical, novel and original contributions investigating but not limited to the following:

- Secure Remote Access
- Identity Access Management
- Access Management
- Identity Governance and Life Cycle
- Privileged Identity Management
- Application Security
- Data Security
- Content Security
- Transaction Protection
- Fraud Protection

- Criminal Detection
- Attacks on Virtualized Systems
- Attacks on Hardware
- Cloud Security
- Cloud Access Security
- Cognitive Security
- Countermeasures and Security Threats
- Cyber Physical System (CPS) Security
- Cybersecurity and Blockchain Technology
- Database and System Security
- Data Center Network Control, Security and Optimization
- Security Standards, Frameworks and Policies
- E-mail Security, Spam, Phishing, E-mail Fraud
- Internet of Things (IoT) Security
- Internet Security, Applications Security and Network Management
- Intrusion Detection and Prevention
- Network and Wireless Network Security
- Peer-to-Peer Network Security
- Performance Evaluations of Protocols and Security Applications
- Security of Virtual Machines
- Phishing, Scams etc.
- Security, Trust and Privacy Challenges
- Smart City Security
- Smart Grid security
- Ubiquitous Computing Security
- Virus, Worms, Trojan Protection
- Incident Response
- Other similar themes relating to Cybersecurity and COVID-19

Manuscript Preparation and Submission

Before submission, authors should carefully read the journal's "Submission Guidelines" (http://www.ieomsociety.org/journals/authors/). The review process will follow the journal's practice. Prospective authors should submit an electronic copy of their complete manuscript via the manuscript submission link (https://mc04.manuscriptcentral.com/ijieom), according to the following timetable:

List of Important Dates

Non-mandatory Abstract Submission: **3 April 2021**

Manuscript Submission Deadline: **12 October 2021**

Notification of First Decision: 7 **January 2022**

Revised Version Submission: **3 March 2022**

Final Decision: **20 March 2022**

Expected Publication: **First or Second Half of 2022**

For further enquiries, please contact any of the special issue guest editors.

Guest Editors

Dr. Sam Takavarasha Jr. (Managing Guest Editor)
Women's University in Africa, Zimbabwe
E-mail: stakavarasha@wua.ac.zw; stjnr1@gmail.com

Dr. Renier Van Heerden
SANReN Cybersecurity Manager
South African National Research Network (SANReN), CSIR Next Generation
E-mail: renier@sanren.ac.za

Prof. Surendra Colin,
Thakur, Research Chair in Digitalisation
Durban University of Technology, South Africa
E-mail: thakur@dut.ac.za

Prof Annelie Jordaan
South African Technology and Training Platform (SATTP), South Africa
E-mail: annelie.jordaan@sattp.net