big data and cognitive computing

Editorial

Managing Cybersecurity Threats and Increasing Organizational Resilience

Peter R. J. Trim [1,*] and Yang-Im Lee [2,*]

[1] Birkbeck Business School, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK
[2] Westminster Business School, University of Westminster, 35 Marylebone Road, London NW1 5LS, UK
* Correspondence: p.trim@bbk.ac.uk (P.R.J.T.); y.lee@westminster.ac.uk (Y.-I.L.)

Cyber security is high up on the agenda of senior managers in private and public sector organizations and is likely to remain so for the foreseeable future. Because cyber-attacks are increasing in sophistication and are of a persistent nature, it is clear that those undertaking research into counteracting cyber threats should familiarize themselves with the types of vulnerability that are likely to be exploited and develop workable solutions. This means working with likeminded people that are intent on ensuring that those carrying out such attacks do not succeed. It is because of the complexity and width of the problem that it is unlikely that those working in a single discipline will be able to solve the recurring problems that managers face. Indeed, the nature of connectivity and interactivity requires that cyber security researchers adopt an inter-disciplinary and/or multi-disciplinary approach to solving cyber security problems, and also that academic and industry researchers cooperate in order to work on cyber security solutions that can be applied across all industry sectors.

This Special Issue draws on the knowledge of various cyber security experts from a range of disciplines who address a number of issues and put forward solutions that utilize cyber security intelligence, with the aim of making organizations more resilient and able to withstand different types of cyber-attack. This means that studying the problem from various perspectives and establishing the breadth and depth of the problem are key priorities. The collection of papers in this Special Issue will help broaden the scope of the subject matter and through interpretation will offer recommendations for dealing with known cyber threats.

This volume of papers complements the existing literature and places cybersecurity within a wider context so that various concepts, models, and strategies can be applied to solving cybersecurity threats as and when they occur. Indeed, in [1] the vulnerability of individuals is made clear, and this is due to the increasing use of social media platforms and the increase in electronic risks that have allowed cybercrime to thrive. To counteract phishing and various other forms of cyber-attack, attention to data privacy is essential. This means that cyber security awareness is given priority and ways are found to reduce individuals' vulnerabilities. In [2], reference is made to ransomware attacks, which result in monetary losses and reputational damage, and it is for these reasons that current trends need to be monitored and ransomware detection deployed. By having an overview of ransomware attacks, intelligence can be established that identifies and minimizes the actions of those carrying out such attacks.

As regards security threats and requirements, Ref. [3] advocates a data processing approach that outlines the steps incorporated within a centralized contact tracing system that can prove beneficial in terms of collecting and sharing information relating to an event/outcome. By mapping security and privacy threats, the security requirements for each type of threat can be made known and the centralized contact tracing system can be viewed as effective. Acknowledging that decision support tools play a useful role vis à vis intelligent sociotechnical systems [4], a number of challenges can be overcome. The emphasis is on the ability to analyze and process various forms of information. Defeasible

check for updates

Citation: Trim, P.R.J.; Lee, Y.-I. Managing Cybersecurity Threats and Increasing Organizational Resilience. *Big Data Cogn. Comput.* **2023**, *7*, 177. https://doi.org/10.3390/bdcc7040177

Received: 15 November 2023
Accepted: 16 November 2023
Published: 22 November 2023

logic programming (DeLP) can be utilized, a P-DAQAP framework can be developed, and a preliminary empirical evaluation undertaken.

Reflecting on the fact that security controls help to safeguard software [5], it is essential to find novel alternatives such as Security Chaos Engineering (SCE) that can be used to protect assets. A defensive security strategy can harness ChaosXploit, which will help identify and correct software misconfigurations sooner rather than later. Accepting that 5G communications systems are vulnerable [6], it can be argued that it is necessary to establish and measure the primary indicators in relation to the effectiveness of a security system, devise a list of cybersecurity KPIs, and model matters accordingly. Additionally, critical infrastructure can be better protected through the deployment of Threat Hunters that are able to detect anomalies [7]. Artificial intelligence (e.g., machine learning) and visualization techniques can enhance Cyber Situational Awareness (CSA) and manifest in the protection of critical infrastructure.

A particle swarm optimization (PSO)-driven selection approach to identify the optimum feature subsets and hybrid ensemble can help to enhance anomaly-based intrusion detection systems [8]. Research [9] undertaken into deep learning to detect and protect against botnet threats in relation to flying ad hoc networks (FANETs) utilizes the hybrid shark and bear smell optimization algorithm (HSBSOA). The outcome is the hybrid shark and bear smell-optimized dilated convolutional autoencoder (HSBSOpt_DCA).

In [10], a solution is provided for the transfer between blockchain-based heterogeneous cryptocurrencies and central bank digital currencies (CBDCs). The researchers focus on and draw from existing interoperability studies and solutions. An interoperable architecture involving heterogeneous blockchains is used, and a decentralized peer-to-peer (P2P) service model is proposed. In addition, security threats to the proposed service model are made known and, most importantly, security requirements to counteract security threats are detailed. In [11], attention is given to how managers can better appreciate the role that sociocultural intelligence plays and utilize artificial intelligence more to facilitate cyber threat intelligence (CTI). The intelligence cycle (IC) and the critical thinking process (CTP) are described and combined, and a cyber threat intelligence cycle process (CTICP) is developed that aids the resilience-building process.

Reflecting on the above set of papers, it can be argued that much has been achieved as regards counteracting the actions of those intent on carrying out cyber-attacks, but there is still a lot more work to be done. Clearly, the benefits of adequate cyber security provision are clear to see, and the holistic picture derived from this Special Issue will help to identify new areas of research and foster continued cooperation among cybersecurity researchers. This is important for strengthening the academic base of the subject and encouraging researchers from academia, industry, and government to pool resources and find novel solutions to current and emerging forms of cyber-attack.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alrobaian, S.; Alshahrani, S.; Almaieh, A. Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. *Big Data Cogn. Comput.* **2023**, *7*, 73. [CrossRef]
2. Alraizza, A.; Algarni, A. Ransomware detection using machine learning: A survey. *Big Data Cogn. Comput.* **2023**, *7*, 143. [CrossRef]
3. Park, S.; Youm, H.-Y. Security and privacy threats and requirements for the centralized contact tracing systems in Korea. *Big Data Cogn. Comput.* **2022**, *6*, 143. [CrossRef]
4. Leiva, M.A.; García, A.J.; Shakarian, P.; Simari, G.I. Argumentation-based query answering under uncertainty with application to cybersecurity. *Big Data Cogn. Comput.* **2022**, *6*, 91. [CrossRef]
5. Chavarro, S.P.; Nespoli, P.; Díaz-López, D.; Roa, Y.N. On the way to automatic exploitation of vulnerabilities and validation of systems security through security chaos engineering. *Big Data Cogn. Comput.* **2023**, *7*, 1.
6. Odarchenko, R.; Iavich, M.; Iashvili, G.; Fedushko, S.; Syerov, Y. Assessment of security KPIs for 5G network slices for special groups of subscribers. *Big Data Cogn. Comput.* **2023**, *7*, 169. [CrossRef]
7. Lozano, M.A.; Llopis, I.P.; Domingo, M.E. Threat hunting architecture using a machine learning approach for critical infrastructure protection. *Big Data Cogn. Comput.* **2023**, *7*, 65. [CrossRef]

8. Louk, M.H.L.; Tama, B.A. PSO-driven feature selection and hybrid ensemble for network anomaly detection. *Big Data Cogn. Comput.* **2022**, *6*, 137. [CrossRef]
9. Abdulsattar, N.F.; Abedi, F.; Ghanimi, H.M.A.; Kumar, S.; Abbas, A.H.; Abosinnee, A.S.; Alkhayyat, A.; Hassan, M.H.; Abbas, F.H. Botnet detection employing a dilated convolutional autoencoder classifier with the aid of hybrid shark and bear smell optimization algorithm-based feature selection in FANETs. *Big Data Cogn. Comput.* **2022**, *6*, 112. [CrossRef]
10. Park, K.; Youm, H.-Y. Proposal of decentralized P2P service model for transfer between blockchain-based heterogeneous cryptocurrencies and CBDCs. *Big Data Cogn. Comput.* **2022**, *6*, 159. [CrossRef]
11. Trim, P.R.J.; Lee, Y.-I. Combing sociocultural intelligence with artificial intelligence to increase organizational cyber security provision through enhanced resilience. *Big Data Cogn. Comput.* **2022**, *6*, 110. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.