

## บรรณานุกรม

- กระทรวงพลังงาน. (2560). ความจำเป็นของการบริหารความต่อเนื่องทางธุรกิจ. [สืบค้นเมื่อ Oct 28, 2017]. Available from : [http://www.doeb.go.th/kmv2/news/Business\\_Continuity\\_55.pdf](http://www.doeb.go.th/kmv2/news/Business_Continuity_55.pdf).
- กิตติพงษ์ จิรวังวงศ์. (2012). ISO 22301 มาตรฐานระบบบริหารความต่อเนื่องทางธุรกิจ. **For Quality**, 182, 13-15.
- กัลยา วานิชย์บัญชา. (2549). การใช้ SPSS for Windows ในการวิเคราะห์ข้อมูล. พิมพ์ครั้งที่ 8. กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย .
- กัลยา วานิชย์บัญชา. (2549). สถิติสำหรับงานวิจัย. พิมพ์ครั้งที่ 2. กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.
- เกริกเกียรติ ศรีเสริมโภค. การบริหารแบบมุ่งผลสัมฤทธิ์ (Performance Management). [สืบค้นเมื่อ เมษายน 25, 2560]. Available from: <https://www.siamhrm.com/?name=hr&file=read&max=590>.
- เกริกเกียรติ ศรีเสริมโภค. สมรรถนะกับการบริหารทรัพยากรบุคคล (Competency – based Human Resource Management). [สืบค้นเมื่อ เมษายน 25, 2560], Available from: <https://slideplayer.in.th/slide/14551022/>.
- ครรชิต มาลัยวงศ์. (2547). แนวทางการนำแบบจำลองวุฒิความสามารถด้านซอฟต์แวร์มาใช้ในองค์กร. [สืบค้นเมื่อ มีนาคม, 2559]. Available from: <http://207.44.134.110/~admin16/books/articles/cmm-in-office.pdf>.
- จิรประภา อัครบวร. (2549). สร้างคนสร้างผลงาน. กรุงเทพมหานคร: ก.พลพิมพ์ (1996).
- ชูชัย สมितिไกร. (2550). การสรรหา การคัดเลือก และการประเมินผล การปฏิบัติงานของบุคลากร. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.
- ณรงค์วิทย์ แสนทอง. (2547). มารู้จัก COMPETENCY กันเถอะ. กรุงเทพมหานคร: เอช อาร์ เซ็นเตอร์.
- ธานี จิตรรั้ว และสำรวม จงเจริญ. (2559). การเปรียบเทียบประสิทธิภาพของสถิติทดสอบในการทดสอบความสมมาตรของการแจกแจงด้วยวิธีการสถิติแบบไม่อิงพารามิเตอร์. **วารสารวิทยาศาสตร์และเทคโนโลยี**. 24(5-ฉบับพิเศษ).
- นงลักษณ์ วิรัชชัย. (2542). โมเดลลิสมเรล : สถิติวิเคราะห์สำหรับการวิจัย, พิมพ์ครั้งที่ 3. กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

- ปรัชญา เถลิมนวัฒน์. (2561). แนวทางการพัฒนากาลังพลด้านไซเบอร์ เพื่อพร้อมรับภัยคุกคามระดับชาติ. วิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561.
- ญงพล บินกาญจน์ และศิริกัญญา ตันสกุล. (2557). ข้อสังเกตและข้อเสนอนโยบาย Digital Economy. รายงานผลการศึกษา มูลนิธิสถาบันอนาคตไทยศึกษา, 1–5.
- ยุทธนา เจียมตระการ. (2561). การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่. วิทยาลัยป้องกันราชอาณาจักร หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60 ประจำปีการศึกษา พุทธศักราช 2560 – 2561.
- ลัดดาวัลย์ เพชรโรจน์ และอัจฉรา ธานีประศาสน์. (2545). ระเบียบวิธีการวิจัย. กรุงเทพฯ: พิมพ์ดีการพิมพ์.
- ศุภศิลป์ กุลจิตต์เจือวงศ์. (2012). 2022 วิวัฒนาการการสื่อสารแห่งโลกอนาคต. *Veridian E-Journal*, 5(2).
- สภการบริหารจัดการภัยพิบัติกลาง คณะสอบสวนพิเศษด้านการปรับปรุงการบริหารจัดการภัยพิบัติ. (2560). การลดผลกระทบจากภัยพิบัติและการปรับปรุงรับมือกับภัยพิบัติโดยบริษัทญี่ปุ่น. Asian Disaster Reduction Center (ADRC). [สืบค้นเมื่อ 28 ตุลาคม 2560], Available from: [http://www.adrc.asia/publications/psdrr/pdf/Guideline\\_Thai.pdf](http://www.adrc.asia/publications/psdrr/pdf/Guideline_Thai.pdf)
- สุชาติพิศ เลิศวิวัฒน์ชัยพร และคณะ. (2561). การบริหารจัดการโลจิสติกส์และโซ่อุปทานให้กับเกษตรกรชาวนาแก้ว จังหวัดสุพรรณบุรี. รายงานฉบับสมบูรณ์ คณะบริหารธุรกิจและเทคโนโลยีสารสนเทศ, มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ.
- สุชาติเทพ รุณเรศ. (2561). ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. การค้นคว้าอิสระ สาขานโยบายและการบริหารเทคโนโลยีสารสนเทศ วิทยาศาสตร์ มหาบัณฑิต วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.
- สุกมาส อังสุโชติ, สมถวิล วิจิตรวรรณ และรัชนิกุล ภิญโญภาณุวัฒน์. (2554). สถิติวิเคราะห์สำหรับการวิจัยทางสังคมศาสตร์และพฤติกรรมศาสตร์: เทคนิคการใช้โปรแกรม LISREL. พิมพ์ครั้งที่ 3. กรุงเทพฯ: เจริญดีมั่นคงการพิมพ์.
- สุรินทร์ นียมางกูร. (2548). สถิติวิจัย. พิมพ์ครั้งที่ 2. กรุงเทพฯ: มหาวิทยาลัยเกษตรศาสตร์.
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2561). นโยบายและแผนระดับชาติว่าด้วย การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 – 2580). กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

- สำนักงานคณะกรรมการพัฒนาระบบราชการ ก.พ.ร. (2560). **คู่มือการบริหารจัดการความพร้อมต่อสถานะวิกฤติ**. สำนักงานคณะกรรมการพัฒนาระบบราชการ. [สืบค้นเมื่อ 28 ตุลาคม 2560]. Available from: [https://www.opdc.go.th/lite/book\\_bcmup.pdf](https://www.opdc.go.th/lite/book_bcmup.pdf).
- สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.). **สสว. รับมอบนโยบายส่งเสริม SMEs พร้อมเดินหน้านำงานปี 2559**. [สืบค้นเมื่อ 18 มิถุนายน 2559], Available from: <http://www.sme.go.th/th/index.php/news1/1015-smes-2559>.
- สำนักงานส่งเสริมรัฐวิสาหกิจขนาดกลางและขนาดย่อม. (2560). **การวางแผนความต่อเนื่องทางธุรกิจ**. สำนักงานส่งเสริมรัฐวิสาหกิจขนาดกลางและขนาดย่อม. [สืบค้นเมื่อ 28 ตุลาคม 2560]. Available from: <http://www.sme.go.th/.../บทความเดือนมีนาคม%20Business%20Continuity%20Plan.pdf>.
- ศิริชัย กาญจนวาสี. (2545). **สถิติประยุกต์สำหรับการวิจัย**. (พิมพ์ครั้งที่ 3). กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.
- ศิลปพร ศรีจันเพชร. (2554). **การบริหารความเสี่ยง: กลไกการกำกับดูแลกิจการ**. วารสารบริหารธุรกิจ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์, 130, 1-3.
- เศรษฐพงศ์ มะลิวรรณ. **ภัยคุกคามรูปแบบใหม่ Cyber Attack**. [สืบค้นเมื่อ มกราคม 2016]. Available from: <http://www.vcharkarn.com/varticle/40535>.
- อริพงษ์ ฤทธิชัย. **แนวคิดเรื่องสมรรถนะ**. [สืบค้นเมื่อ 25 เมษายน 2560]. Available from: <http://www.jobpub.com/articles/showarticle.asp?id=2213>.
- อมาวลี อัมพันศิริรัตน์. (2557). **มโนทัศน์ของการวิจัยเชิงคุณภาพ**. วารสารเครือข่ายวิทยาลัยพยาบาลและการสาธารณสุขภาคใต้. 1(2), 68 - 80.
- เอี่ยมพร หลินเจริญ. (2555). **เทคนิคการวิเคราะห์ข้อมูลเชิงคุณภาพ**. วารสารการวัดผลการศึกษามหาวิทยาลัยมหาสารคาม, 17(1), 17-29.

## BIBLIOGRAPHY

- Abderrahim, W., & Choukair, Z. (2017). The three-dimensional model for dependability integration in cloud computing. **Annals of Telecommunications**, 72(5-6), 371–384.
- Akinrolabu, O., New, S., & Martin, A. (2017). Cyber supply chain risks in cloud computing bridging the risk assessment gap. **Open Journal of Cloud Computing**, 5(1), 1–19.
- Al-Shboul, M. (2017). Infrastructure framework and manufacturing supply chain agility: the role of delivery dependability and time to market. **Supply Chain Management: An International Journal**, 22 (2), 172-185.
- Allan, N., Zhang, Mark, G., & Fanwen, M. (2010). Conceptual modelling for supply chain inventory visibility. **International of Production Economics**, 133 (2), 578–585.
- Alexander, A.G., Phuoc Q., Mahesh, P., Zachary A.C., Jeffrey M.K. Dayton, M., & Igor, L. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. **Risk Analysis: An International Journal**.
- Ali, M., Tatiana, B., & Michael, M. (2013). An Effective Method For Information Security Awareness Raising Initiatives. **International Journal of Computer Science & Information Technology (IJCSIT)**, 5 (2), 63-72.
- Alsadhan, T., & Park, J. S. (2016, June). Security Automation for Information Security Continuous Monitoring: Research Framework. **2016 IEEE World Congress on Services (SERVICES)**. (pp. 130-131). IEEE.
- Amin, R., Islam, S. H., Kumar, N., & Choo, K. K. R. (2018). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. **Journal of Network and Computer Applications**, 104, 133–144.

- Anantadjaya, S., Walidin, A., Waskita, E.S., & Nawangwulan, I. M. (2007, August). Consumer Behavior, Supply Chain Management and Customer Satisfaction : An Investigative Study in Small and Medium Enterprise. In **Supply Chain Management and Customer Satisfaction: An Investigative Study in Small and Medium Enterprise (August 30, 2007). Proceeding, International Seminar on Industrial Engineering and Management.**
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. **MIS Quarterly**, 34(3), 613-643.
- Andreasson, K. J. (2011). **Cybersecurity: Public Sector Threats and Responses.** CRC Press.
- Armstrong, S.J., & Overton T.S. (1997). Estimating non-response bias in mail surveys. **Journal of Marketing Research**, 14(3), 396-402.
- Aron, R., Clemons, E. K., & Reddi, S. (2012). Just right outsourcing: Understanding and managing risk. **Journal of management information systems**, 22(2), 37-55.
- Asbjørnslett, B.E. (2009). Assessing the vulnerability of supply chains. In: **Supply Chain Risk.** (pp. 15-33). Springer, Boston, MA.
- Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. **Information Management & Computer Security**, 22 (3), 251-264.
- Australian Signals Directorate (ASD). (2017, February). Strategies to Mitigate Cyber Security Incidents – Mitigation Details. **Australian Cyber Security Center.**
- Aviles, M. E. (2015). **The Impact of Cloud Computing in Supply Chain Collaborative Relationships, Collaborative Advantage and Relational Outcomes.** Electronic Thesis & Dissertations. Paper 1244.
- Avizienis, A. (1967, November). Design of fault-tolerant computers. In **Proceedings of the November 14-16, 1967, fall joint computer conference** (pp. 733-743).
- Avizienis A., & Chen, L. (1977, November). On the implementation of N-version programming for software fault tolerance during execution. In **Proc. IEEE COMPSAC 77** (pp. 149 -155).
- Avizienis, A., Laprie, J. C., & Randell, B. (2001). **Fundamental concepts of dependability.** University of Newcastle upon Tyne, Computing Science (pp. 7- 12).

- Azarnik, A., Shayan, J., Alizadeh, M., Karamizadeh, S., (2012). Associated Risks of Cloud Computing for SMEs. **Open International Journal of Informatics (OIJI)**, 1, 37-45.
- Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. **International Journal of Information Management**, 43, 76–84.
- Bak, O. (2018). Supply chain risk management research agenda: From a literature review to a call for future research directions. **Business Process Management Journal**, 24(2), 567-588.
- Bakshi, N., & Kleindorfer, P. (2009). Co-operation and investment for supply-chain resilience. **Production and Operations Management**, 18(6), 583-603.
- Banomyong, R. (2018). **Collaboration in Supply Chain Management: A Resilience Perspective**. International Transport Forum Discussion Paper, no.2018-22.
- Barbara, G., & Giorgia, S. (2017). Managing IT and Cyber Risks in Supply Chains. **Supply Chain Risk Management**, (pp. 85-96). Springer, Singapore.
- Barratt, M. (2004). Understanding the meaning of collaboration in the supply chain. **Supply Chain Management: An International Journal**, 9(1), 30 - 42.
- Beamon, B.M. (1999). Measuring supply chain performance. **International Journal of Operations & Production Management**, 19(3), 275-292.
- Becky Maycock. (2010). Communication Strategies for Incident Response (Mass Notification and Beyond). **Impact Technologies, Inc.**
- Bechthold, J. (2014). Industry 4. 0. The capgemini consulting view, sharpening the picture beyond the hype. **Capgemini Consulting**.
- Besnard, D. & Arief, B. (2017). Computer Security Impaired by Legitimate Users. **Computers & Security**, 23, 253-264.
- Bhargava, B., Ranchal, R. and BenOthmane, L. (2013). Secure information sharing in digital supply chains. In **2013 3<sup>rd</sup> IEEE International Advance Computing Conference (IACC)** (pp. 1636–1640). IEEE.

- Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016, September). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In **Annual Privacy Forum** (pp. 21-37). Springer, Cham.
- Blackhurst, J., Kaitlin, S.D. & Craighead, C.W. (2011). An empirically derived framework of global supply resiliency. **Journal of Business Logistics**, 32(4), 374-391.
- Bollen, K.A. (1989). *Structural Equations with Latent Variables* Wiley. **New York**.
- Bonkenburg, T. (2016). Robotics in logistics. **A DPDDHL perspective on implications and use cases for the logistics industry. DHL Trend Research, 1**.
- Borrett, M., Carter, R. & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider?. **Journal of Business Continuity & Emergency Planning**, 7 (1), 163-171.
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. **Technovation**, 34 (7), pp. 342–353.
- Brar, H. S., & Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. **Journal of Computer Networks and Communications**, 2018.
- Braunscheidel, M.J. & Suresh, N.C. (2009). The organizational antecedents of a firm's supply chain agility for risk mitigation and response. **Journal of Operations Management**, 27(2), 119-140.
- Bryndin E. (2018). Directions of Development of Industry 4.0, Digital Technology and Social Economy. **American Journal of Information Science and Technology**, 2(1), 9-17.
- Bouricius, W.G., Carter, J. C., & Schneider, P.R. (1969). Reliability modeling techniques for self repairing computer systems. In **Proceedings of the 1969 24<sup>th</sup> National Conference** (pp. 295 – 309).
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. **Technovation**, 34 (7), 342–353.
- Bukowski, L. (2016). System of systems dependability – Theoretical models and applications examples. **Reliability Engineering & System Safety**, 151, 76–92.

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **MIS Quarterly**, 334 (3), 523-548.
- Busse, C., Meinschmidt, J., Foerstl, K. (2016). Managing Information Processing Needs in Supply Chains: A Prerequisite to Sustainable Supply Chain Management. **Journal of Supply Chain Management**, 53(1), pp. 87 - 11.
- Büyüközkan, G., & Göçer, F. (2018). Digital Supply Chain: Literature review and a proposed framework for future research. **Computers in Industry**, 97, 157–177.
- Bryndin, E. (2018). Directions of Development of Industry 4.0, Digital Technology and Social Economy. **American Journal of Information Science and Technology**, 2(1), 9-17.
- Cabral, I., Grilo, A. & Cruz-Machado, V. (2012). A decision-making model for lean, agile, resilient and green supply chain management. **International Journal of Production Research**, 50 (17), 4830-4845.
- Cadarso, L., Maroti, G., & Marin, A. (2015). Smooth and Controlled Recovery Planning of Disruptions in Rapid Transit Networks. **IEEE Transactions on Intelligent Transportation Systems**, 16 (4), 2192–2202.
- Cai, J., Liu, X., Xiao, Z. & Liu, J. (2009). Improving supply chain performance management: a systematic approach to analyzing iterative KPI accomplishment. **Decision Support Systems**, 46(2), 512-21.
- Cao, M., & Zhang, Q. (2011). Supply chain collaboration : Impact on collaborative advantage and firm performance. **Journal of Operations Management**, 29 (3), 163–180.
- Cao, M., Vonderembse, M. A., Zhang, Q., & Ragu-Nathan, T.S. (2010). Supply chain collaboration: conceptualisation and instrument development. **International Journal of Production Research**, 48(22), 6613–6635.
- Carvalho, H., Duarte, S. & Machado, V. C. (2011). Lean, agile, resilient and green: divergencies and synergies. **International Journal of Lean Six Sigma**, 2(2), 151 – 179.
- Carvalho, H., Barroso, A.P., Machado, V.H., Azevedo, S. & Cruz-Machado, V. (2012). Supply chain redesign for resilience using simulation. **Computers & Industrial Engineering**, 62 (1), 329-341.



- Cecere, L. (2016). **Embracing the Digital Supply Chain**. [Retrieved October 15, 2016]. Available from: <http://www.supplychainshaman.com/demand/demanddriven/embracing-the-digital-supply-chain/>.
- CERT. (2013). **2013 US State of Cybercrime Survey**. [Retrieved March 15, 2020]. Available from: [http://resources.sei.cmu.edu/asset\\_files/Presentation/2013\\_017\\_101\\_58739.pdf](http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf).
- Cepel, M., Stasiukynas, A., Kotaskova, A., & Dvorsky, J. (2018). Business Environment Quality Index in the SME Segment. *Journal of Competitiveness*, 10 (2), 21-40.
- Chan, F.T.S. (2003). Performance measurement in a supply chain. *International Journal of Advanced Manufacturing Technology*, 21(7), 534-548.
- Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. *Big Data Research*, 3, 10–23.
- Chemweno, P., Pintelon, L., Muchiri, P. N., & Van Horenbeek, A. (2018). Risk assessment methodologies in maintenance decision making: A review of dependability modeling approaches. *Reliability Engineering & System Safety*, 173, 64–77.
- Chen, J. V., Yen, D. C., Rajkumar, T. M., & Tomochko, N. A. (2011). The antecedent factors on trust and commitment in supply chain relationships. *Computer Standards & Interface*, 33(3), 262–270.
- Chen, LM., Liu, YE., & Yang, SJS. (2015). Robust supply chain strategies for recovering from unanticipated disasters. *Transportation Research Part E: Logistics and Transportation Review*, 7, 198-214.
- Chen Y. and A. Bharadwaj, (2009). An Empirical Analysis of Contract Structures in IT Outsourcing. *Information System Research*, 20, 484-506.
- Chen, Z. & Suhong, L. (2006). Secure Information Sharing in Internet Based Supply Chain Management Systems. *Journal of Computer Information Systems*, 46 (4), 18-24.
- Chhetri, S. R., Faezi, S., Rashid, N., & Al Faruque, M. A. (2017). Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. *Journal of Hardware and Systems Security*. 2(1), 51–68.

- Chkanikova, O. (2012). Sustainable Supply Chain management: theoretical literature overview. Sweden: **International Institute for Industrial Environmental Economics, Lund University.**
- Choo, K. K. R. (2014). A conceptual interdisciplinary plug-and-play cyber security framework. In **ICTs and the Millennium Development Goals** (pp. 81-99). Springer, Boston, MA.
- Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. **International Journal of Computer Science & Information Technology**, 5(3), pp. 79.
- Christine T. B., & Ronald L. B. (2018). An initial assessment of small business risk management approaches for cyber security threats. **International Journal Business Continuity and Risk Management**, 8(1), 1-10.
- Christopher, M. & Peck, H. (2004). Building the resilient supply chain. **The International Journal of Logistics Management**, 15(2), 1-13.
- Chuan, P., Khachidze, V., Lai, I. K. W., Liu, Y., Siddiqui, S., & Wang, T. (Eds.). (2013). Multi-level Access Control in the Data Pipeline of the International Supply Chain System. In **Innovation in the High-Tech Economy** (pp. 79-90). Springer, Berlin, Heidelberg.
- Chunghun, L., Choong, C.L., & Suhyun, K. (2016). Understanding information security stress: focusing on the type of information security compliance activity. **Computers & Security**, 59, 60-70.
- Cienfuegos, J. S. (2013). **Developing a Risk Management Maturity Model**. Dissertation of the degree of doctor at the Department of Public Administration, Institute for Innovation and Governance Studies, Faculty of Management and Governance, University of Twente.
- Cirulis, A. and Ginters, E. (2013). Augmented reality in logistics, **Procedia Computer. Science**, 26(11), 14–20.
- Cisco. (2015). **Cisco Study: IT Saying Yes to BYOD**. [Retrieved March 05, 2020]. Available from: <http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD>.
- Claudine A., Soosay, P. W., Hyland, M. F. (2008). Supply chain collaboration: capabilities for continuous innovation. **Supply Chain Management: An International Journal**, 13(2), 160 – 169.

- Clemons E. K. and L. M. Hitt, (2017). Poaching and the Misappropriation of Information: Transaction Risks of Information Exchange. **Journal of Management Information System**, 21(2), 87-107.
- Colicchia, C., Dallari, F., & Melacini, M. (2010). Increasing supply chain resilience in a global sourcing context. **Production Planning & Control**, 21(7), 680-694.
- Colin, P., Gabriela, A., & Hugh, W. (2012). The governance of supply networks: a systematic literature review. **Supply Chain Management: An International Journal**, 17(4), 358-376.
- Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity Standards: Managing Risk and Creating Resilience. **Computer**, 47(9), 70–76.
- Computer World, UK. (2015). **European Firms Allow BYOD Despite Security Concerns**. [Retrieved February 23, 2020]. Available from: <https://www.computerworlduk.com/news/mobile-wireless/3359491/european-firms-allow-byod-despite-security-concerns>.
- Crook, T. R., Giunipero, L., Reus, T. H., Handfield, R., & Williams, S. K. (2008). Antecedents and Outcomes of Supply Chain Effectiveness : An Exploratory Investigation. **Journal of Managerial Issues**, 20(2), 161-177.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. **Computers & Security**, 32, 90–101.
- Cruz, T., Rosa, L., Proenca, J., Maglaras, L., Aubigny, M., Lev, L., & Simoes, P. (2016). A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems. **IEEE Transactions on Industrial Informatics**, 12(6), 2236–2246.
- Cukier, K. (2018). Big data and the future of business. In **the book Reinventing the Company in the Digital Age** (pp. 37–51), 2015.
- Daniel, I. P. (2015). The strategic fit between innovation strategies and business environment in delivering business performance. **International Journal of Production**, 171, 241-249.

- Datta, P.P., Christopher, M. & Allen, P. (2007). Agent-based modelling of complex production/distribution systems to improve resilience. **International Journal of Logistics: Research and Applications**, 10(3), 187-203.
- David, M. G., & Mary, C. H. (2012). Antecedents and Consequences of Supply Chain Agility: Establishing the Link to Firm Performance. **Journal of Business Logistics**, 33(4), 295–308.
- Derek, Y., Juan, L.Jr., Mason, R., Benjamin, R., & Robert, Mc. (2016). A framework for incorporating insurance in critical infrastructure risk strategies. **International Journal of Critical Infrastructure Protection**, 14, 43-57.
- Devos, J., Van Landeghem, H. & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. **Industrial Management & Data Systems**, 112(2), 206-223.
- Dhar, S. (2012). From outsourcing to Cloud computing: evolution of IT services. **Management Research Review**, 35(8), 664 – 675.
- DHL Trend Research. (2014). **Self-Driving Vehicles in Logistics**, DHL Cust. Solut. Innov. [Retrieved March 25, 2019] . Available from: [http://www.dhl.com/content/dam/downloads/g0/about\\_us/logistics\\_insights/dhl\\_self\\_driving\\_vehicles.pdf](http://www.dhl.com/content/dam/downloads/g0/about_us/logistics_insights/dhl_self_driving_vehicles.pdf).
- Dhillon, G., & Torkzadeh, G. (2006). Value-focused Assessment of Information Systems Security in Organizations. **Information Systems Journal**, 16(3), 293-314.
- Diamantopoulos, A., & Siguaw, A.D. (2000). **Introducing LISREL: A guide for the uninitiated**. Sage Publications, London.
- Discussion Papers. (2011). **Developing A Response Analysis Framework**. Food and Agriculture Organization of the United Nations, Rome, 2011.
- Dobson, J. E., & Randell, B. (2001, December). Building reliable secure computing systems out of unreliable insecure components. In **Seventeenth Annual Computer Security Applications Conference** (pp. 164-173). IEEE.
- Dolci, P., Maçada, A. and Paiva, E. (2017). Models for understanding the influence of Supply Governance on Supply Chain Performance. **Supply Chain Management: An International Journal**, 22(5), 424-441.

- Dong, S., Xu, S. X., & Zhu, K. X. (2009). Information Technology in Supply Chains: The Value of IT-Enabled Resources Under Competition. **Information Technology in Supply Chains : Information Systems Research**, 20(1), 18–32.
- Dmitry, I., Alexandre, D., & Boris, S. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. **International Journal of Production Research**, 57(3), 829-846.
- Draft Working. (2019). **National Response Framework 4<sup>th</sup> Edition**. Homeland Security , May 2019.
- Dubey, R., Gunasekaran, A., Papadopoulos, T., Childe, S. J., Shibin, K. T., & Wamba, S. F. (2017). Sustainable supply chain management: framework and further research directions. **Journal of Cleaner Production**, 142, 1119–1130.
- Duffy, J. (2001). Maturity models: Blueprints for evolution. **Strategy & Leadership**, 29(6), 19-26.
- Durach, C. F., Wieland, A., & Machuca, J. A. D. (2015). Antecedents and dimensions of supply chain robustness: a systematic literature review. **International Journal of Physical Distribution & Logistics Management**, 45(1/2), 118–137.
- Durowoju, O. A., Chan, H. K., Wang, X. (2011). The Impact of Security and Scalability of Cloud Service on Supply Chain Performance. **Journal of Electronic Commerce Research**, 12(4), 243-256.
- Durgin, M. (2017). **Understanding the Importance of and Implementing Internal Security Measures**, SANS Institute Read Room. [Retrieved March 04, 2020]. Available from: [https://www2.sans.org/-reading\\_room/whitepapers/policyissues/901.php](https://www2.sans.org/-reading_room/whitepapers/policyissues/901.php).
- Ellinger, A. E., Natarajathinam, M., Adams, F. G., Gray, J. B., Hofman, D., & O'Marah, K. (2011). Supply Chain Management Competency and Firm Financial Success. **Journal of Business Logistics**, 32(3), 214–226.
- Espadinha-Cruz, P. (2012). **Lean, Agile, Resilient and Green Supply Chain Management Interoperability Assessment Methodology**. UNIDEMI, Departamento de Engenharia Mecânica e Industrial, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa.

- Evgeny, L. (2011). **Guide to Developing a Cyber Security and Risk Mitigation Plan**. The National Rural Electric Cooperative Association's Cooperative Research Network.
- Fadeel, S., Felix, O. B. (2016). A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises. **International Journal of Electrical and Computer Engineering (IJECE)**, 6(5), 2425-2431.
- Farahani, P., Meier, C., & Wilke, J. (2017). Digital supply chain management agenda for the automotive supplier industry. In **Shaping the digital enterprise** (pp. 157-172). Springer, Cham.
- Fawcett, S. E., Wallin, C., Allred, C., Fawcett, A. M., & Magnan, G. M. (2011). Information Technology as an Enabler of Supply Chain Collaboration: A Dynamic-Capabilities Perspective. **Journal of Supply Chain Management**, 47(1), 38-56.
- Fawcett, Stanley E., Gregory M. M., & Matthew W. M. (2008). A Three-Stage Implementation Model for Supply Chain Collaboration. **Journal of Business Logistics**, 29(1), 93-112.
- Fayezi, S., Zutshi, A., & O'Loughlin, A. (2016). Understanding and Development of Supply Chain Agility and Flexibility: A Structured Literature Review. **International Journal of Management Reviews**, 19(4), 379-407.
- Fiksel, J. (2006). Sustainability and resilience: toward a systems approach. **Sustainability : Science, Practice, & Policy**, 2(2), 14-21.
- FireEye. (2016). **5 reasons cyber attackers target SMEs**. [Retrieved February 25, 2020]. Available from: <https://www.fireeye.com/-content/-dam/fieeyewww/global/en/offers/-pdfs/SME-Infographicweb.pdf>
- Florian, K. S. S. (2014). Linking Collaboration and Integration to Risk and Performance in Supply Chains via a Review of Literature Reviews. **Supply Chain Management: An International Journal**, 19(5/6).
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. **Computers & Security**, 61, 169-183.
- Forslund, H. (2010). ERP systems' capabilities for supply chain performance management. **Industrial Management & Data Systems**, 110(3), 351 - 367.

- Forslund, H., & Jonsson, P. (2009). Obstacles to supply chain integration of the performance management process in buyer-supplier dyads The buyers' perspective. **International Journal of Operations & Production Management**, 29(1), 77-95.
- Franziska, F., Shellee, W.A., Howard, V., & Levy, C. (2005). **Digital Asset Management-A Closer Look at the Literature**. A Research Monograph of the Printing Industry Center at RIT Rochester, NY March 2005.
- Fray, J.M., Deswarte Y., & Powell D. (1986, April). Intrusion tolerance using fine-grain fragmentation scattering. In **1986 IEEE Symposium on Security and Privacy** (pp. 194-194). IEEE.
- Fredrik, B., Martin, H., Janis, S., & Jelena, Z. (2015). Cyber Resilience – Fundamentals for a Definition. In **New Contributions in Information Systems and Technologies** (pp. 311-316). Springer, Cham.
- Friday, D., Ryan, S., Sridharan, R. & Collins, D. (2018). Collaborative risk management: a systematic literature review. **International Journal of Physical Distribution & Logistics Management**, 48(3), 231-253.
- Galligan, M. E., (2014). **Facing Cyber Threats: Keys to Security, Vigilance, And Resilience**. NACD Directorship March/April 2014, p.62.
- Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). **Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political**. **IEEE Technology and Society Magazine**, 30(1), 28-38.
- Garcia, R. H. & Giachetti, R. (2010). Using experts to develop a supply chain maturity model in Mexico. **Supply Chain Management: An International Journal**, 15(6), 415-424.
- Gaudenzi, B., & Siciliano, G. (2017). Managing IT and Cyber Risks in Supply Chains. **Supply Chain Risk Management** (pp. 85–96). Springer, Singapore.
- George, L., Diane, G., & Tuan, V. (2013). A Review of Cyber Threats and Defence Approaches in Emergency Management. **Future Internet**, 5, 205-236.
- Ghafir, I., & Prenosil, V. (2016). Proposed approach for targeted attacks detection. In **Advanced Computer and Communication Engineering Technology** (pp. 73-80). Springer, Cham.

- Ghafir, I., Prenosil, V., Svoboda, J., & Hammoudeh, M. (2016, August). A survey on network security monitoring systems. In **2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)** (pp. 77-82). IEEE.
- Giannakis, M., & Papadopoulos, T. (2016). Supply chain sustainability: A risk management approach. **International Journal of Production Economics**, 171, 455–470.
- Glockner, H., Jannek, K., Mahn, J. and Theis, B. (2014). Augmented Reality. **Communications of the ACM**, 57(9), 7–7.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2016). **CSI/FBI Computer Crime and Security Survey**. [Retrieved March 04, 2020]. Available from: [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2006.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).
- Golgeci, I. & Ponomarov, S.Y. (2013). Does firm innovativeness enable effective responses to supply chain disruptions? An empirical study. **Supply Chain Management: An International Journal**, 18(6), 604-617.
- Grubisic, I. (2014). ERP in clouds or still below. **Journal of Systems and Information Technology**, 16(1), 62 – 76.
- Gunasekaran, A., Patel, C. & Tirtiroglu, E. (2001). Performance measures and metrics in a supply chain environment. **International Journal of Operations & Production Management**, 21(1/2), 71-87.
- Guanyi, L., Xenophon, K., & Lorenzo, L. (2017). Supply Chain Security : A Classification of Practices and an Empirical Study of Differential Effects and Complementary. **IEEE Transactions on Engineering Management**, 64(2), 234-248.
- Guillén, A. J., Crespo, A., Gómez, J. F., & Sanz, M. D. (2016). A framework for effective management of condition based maintenance programs in the context of industrial development of E-Maintenance strategies. **Computers in Industry**, 82, 170 - 185.
- Hair, J.F., Anderson, R.E., Tatham, R.L., & Black, W.C. (1998). **Multivariate Data Analysis (5th ed)**. Upper Saddle River, NJ: Prentice Hall.
- Hanifan, G., Sharma, A. and Newberry, C. (2014). The Digital Supply Network: A new paradigm for supply chain management.



- Harrison, T. P. (2004). Principles for the strategic design of supply chains. In **The practice of supply chain management: Where theory and application converge** (pp. 3-12). Springer, Boston, MA.
- Härting, R.C., Reichstein, C., & Schad, M. (2018). Potentials of Digital Business Models – Empirical investigation of data driven impacts in industry. **Procedia Computer Science**, 126, 1495–1506.
- Hassell, S., Beraud, P., Cruz, A., & Ganga, G. (2012, October). Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation. In **MILCOM 2012-2012 IEEE Military Communications Conference** (pp. 1-6). IEEE.
- Hawkins, N. (2018). Resistance, response and recovery. **Computer Fraud & Security**, 2018(2), 10–13.
- He, S., Zhu, J., He, P., & Lyu, M. R. (2016, October). Experience Report: System Log Analysis for Anomaly Detection. In **2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE)** (pp. 207-218). IEEE.
- Hearnshaw, E.J.S., & Wilson, M.M.J. (2013). A complex network approach to supply chain network theory. **International Journal of Operations & Production Management**, 33(4), 442-469.
- Heng, G. M. (2015). Business Continuity Management Planning Methodology. **International Journal of Disaster Recovery and Business Continuity**, 6, 9–16.
- Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2012). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. **Information Systems Journal**, 24(1), 61–84.
- Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In **2017 12th Iberian Conference on Information Systems and Technologies (CISTI)** (pp. 1-4). IEEE.
- Hervani, A.A., Helms, M.M., & Sarkis, J. (2005). Performance measurement for green supply chain management. **Benchmarking**, 12(4), 330-353.

- Higgins, A.J.M., Miller, C.J., Archer, A.A., Ton, T., Flecher, C.S., & McAllister, R.R.J. (2010). Challenges of operations research practice in agricultural value chains. **Journal of Operational Research Society**, 61(6), 964-973.
- Hints, J., Gutierrez, X., Wieser, P., & Hameri, A. P. (2009). Supply chain security management: an overview. **International Journal of Logistics Systems and Management**, 5(3), 344-352.
- Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: a literature review. **International Journal of Production Research**, 53(16), 5031–5069.
- Holcomb, M. C., Ponomarev Serhiy Y., & Manrodt Karl B. (2011). The Relationship of Supply Chain Visibility to Firm Performance. **Supply Chain Forum An International Journal**, 12(2), 32-45.
- Hou, Y., Such, J., & Rashid, A. (2019, May). Understanding Security Requirements for Industrial Control System Supply Chains. In **2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)** (pp. 50-53). IEEE.
- Hu, & Bentler. (1999). Cutoff criteria for fit indexes in covariance structure analysis : Coventional criteria versus new alternatives. **Structural equation modeling: a multidisciplinary journal**, 6(1), 1-55.
- Hudnurkar, M., Jakhar, S., & Rathod U. (2013). Factors affecting collaboration in supply chain: A literature Review. **Social and Behavioral Sciences**, 133, 189-202.
- Husdal, J. (2010). A conceptual framework for risk and vulnerability in virtual enterprise networks. In **Managing risk in virtual enterprise networks: implementing supply chain principles** (pp. 1-27). IGI Global.
- Hwang, G. J., Chu, H. n, & Lai, C. L. (2017). Prepare your own device and determination (PYOD): a successfully promoted mobile learning mode in Taiwan. **International Journal of Mobile Learning and Organisation**. 11(2), 87.
- Iakovou, E., Vlachos, D. & Xanthopoulos, A. (2010), A stochastic inventory management model for a dual sourcing supply chain with disruptions. **International Journal of Systems Science**, 41(3), 315-324.
- IBM. (2009). The Smarter Supply Chain of the Future.

- Inderfurth, K., Sadrieh, A., & Voigt, G. (2012). The Impact of Information Sharing on Supply Chain Performance. **Production and Operations Management**, 22(2), 410–425.
- Ishfaq, R. (2012). Resilience through flexibility in transportation operations. **International Journal of Logistics: Research and Applications**, 15(4), 215-229.
- Ismail, G., & Serhiy, Y. P. (2013). Does firm innovativeness enable effective responses to supply chain disruptions? An empirical study. **Supply Chain Management: An International Journal**, 18(6), pp.604 – 617.
- ISO (2010). **ISO/PAS 28002:2010: Security Management Systems for the Supply Chain: Development of Resilience in the Supply Chain**. ISO, Geneva.
- Ivanov, D., Dolgui, A., Sokolov, B., & Ivanova, M. (2017). **Literature review on disruption recovery in the supply chain**. International Journal of Production Research, Vol. 55 Iss. 20, pp. 6158–6174.
- Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. **International Journal of Production Research**, 57(3), 829-846.
- Jairo, R.M.T., & Diego A.O.V.. (2014). **Collaboration and information sharing in dyadic supply chains: A literature review over the period 2000–2012**. Estudios Gerenciales Vol. 30, pp. 343–354
- James, L. Jr., Merrill, W., Robert, E.C. & Robert, F.O. (2017). **Implications of Monitoring Mechanisms on Bring Your Own Device Adoption**. Journal of Computer Information Systems, Vol. 57 Iss. 4, pp. 309-318.
- Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). **Guarding against online threats: why entrepreneurs take protective measures**. Behaviour & Information Technology, Vol. 35 Iss. 5, pp. 368–379.
- Jawad, H.A., Shahzad, M., Rahat, A.K., Abdul, Q.N., Zahoor, H., & Muhammad, U. (2017). **Security strategies to overcome cyber measures, factors and barriers**. Engineering Science And Technology International Research Journal, Vol.1 No.1, pp.51-58.
- Jeske, M., Grüner, M. and WeiB, F. (2013) Big Data in Logistics.

- Jifeng, M., Gang, P., Douglas, L., MacLachlan. (2009). **Effect of risk management strategy on NPD performance.** *Technovation*, Vol. 29 Iss 3, pp. 170-180.
- Johan, S.. (2016). **Secure Tactical Communications for Inter-Organizational Collaboration The Role of Emerging Information and Communications Technology, Privacy Issues, and Cyber Threats on the Digital Battlefield.** Doctoral Dissertation of Skövde, Sweden.
- Johnson, N., Elliott, D., & Drake, P. (2013). **Exploring the role of social capital in facilitating supply chain resilience.** *Supply Chain Management: An International Journal*, Vol. 18 No. 3, pp. 324-336.
- Jones A. (2000). The challenge of building survivable information-intensive systems. **Computer**, 33(8), 39-43.
- Joseph, M.K. & Avizienis A. (1988, April). A fault tolerance approach to computer viruses. In **IEEE Symposium on Security and Privacy** (pp. 52-58).
- Judit, M. (2018). Supply chains robustness: Challenges and opportunities. **Procedia CIRP**, 67, 110 – 115.
- Junho, H. (2014). Integrated Anomaly Detection for Cyber security of the Substations. **IEEE Transactions On Smart Grid**, 5(4), 1643-1653.
- Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: an empirical study. **Supply Chain Management: An International Journal**, 16(4), 246 - 259.
- Kabir, S. (2017). An overview of fault tree analysis and its application in model based dependability analysis. **Expert Systems with Applications**, 77, 114–135.
- Kaie, M., Rain, O., & Olaf, M. (2017, November). Improving and Measuring Learning Effectiveness at Cyber Defense Exercises. In **Nordic Conference on Secure IT Systems** (pp. 123 - 138). Springer, Cham.
- Kalwani, M. U., & Narayanda, N. (1995). Long-Term Manufacturer-Supplier Relationships : Do They pay off for Supplier Firms. **Journal of Marketing**, 59(1), 1-16.
- Kamal, J. (2016). Cyber Risk Assessment in Distributed Information Systems. **The Cyber Defense Review**, 2016, 79-100.

- Kankanhallia, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information Systems Security Effectiveness. **International Journal of Information Management**, 23, 139-154.
- Kaplan, D. (2000). **Structural Equation model: Foundation and extensions**. Sage publications, Thousand Oake.
- Karen, H. (2015). **Enterprise Risk Management : A Guide for Government Professionals**. Jossey-Bass, John Wiley & Sons, Inc.
- Karim, R., Westerberg, J., Galar, D., & Kumar, U. (2016). Maintenance Analytics – The New Know in Maintenance. **IFAC-Papers OnLine**, 49(28), 214–219.
- Karuna, J., & Ashish, D. (2005, January). Supply chain collaboration: A governance perspective. In **Supply Chain Forum: An International Journal** (Vol. 6, No. 2, pp. 50-57). Taylor & Francis.
- Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. **International Journal of Disaster Risk Reduction**, 27, 577–587.
- Kazi Arif-Uz-Zaman, A.M.M., & Nazmul, A. (2014). Lean supply chain performance measurement. **International Journal of Productivity and Performance Management**, 63(5), 588 – 612.
- Keating, A., Venkateswaran, K., Szoenyi, M., MacClune, K., & Mechler, R. (2016). From event analysis to global lessons: disaster forensics for building resilience. **Natural Hazards Earth System Science**, 16(7), 1603–1616.
- Kelley, D., Nirali, S. Chawla, A.J., Ronald J., Alicia, Clay J. A. Orebaugh, M. Scholl, & Kevin, S. (2011). **Information security continuous monitoring (ISCM) for federal information systems and organizations (No. Special Publication (NIST SP) – 800 - 137)**.
- Kenneth, W., Green Jr, P. J., Zelbst Jeremy Meacham Vikram, S. B. (2012). Green supply chain management practices: impact on performance. **Supply Chain Management: An International Journal**, 17(3), 290 – 305.

- Kelly, B.B. (2016). Investing in a centralized cybersecurity infrastructure: Why “hactivism” can and should influence cybersecurity reform. **Boston University Law Review**, 92(5), 1663–1711.
- Kelly Finnerty et al. (2018). **Cyber Security Breaches Survey 2018: Statistical Release**. Cyber security breaches survey 2018: Statistical release.
- Khan, K.A., Bakkappa, B., Metri, B.A., & Sahay, B.S. (2009). Impact of agile supply chains’ delivery practices on firms’ performance: cluster analysis and validation. **Supply Chain Management: An International Journal**, 14(1), 41-48.
- Khatoun, R., & Zeadally, S. (2017). Cybersecurity and Privacy Solutions in Smart Cities. **IEEE Communications Magazine**, 55(3), 51–59.
- Kirstin, S.S.S. (2015). The role of collaboration in supply chain resilience. **Supply Chain Management: An International Journal**, 20(4), 471 – 484.
- Klibi, W., Martel, A., & Guitouni, A. (2010). The design of robust value-creating supply chain networks: a critical review. **European Journal of Operational Research**, 203(2), 283-293.
- Koksal, A., & Ozdemir, A. (2016). Improved transformer maintenance plan for reliability centred asset management of power transmission system. **IET Generation, Transmission & Distribution**, 10(8), 976–1983.
- Komar, M., Kochan, V., Dubchak, L., Sachenko, A., Golovko, V., Bezobrazov, S., & Romanets, I. (2017, September). High performance adaptive system for cyber attacks detection. In **2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)** (Vol. 2, pp. 853-858). IEEE.
- Komljenovic, D., Gaha, M., Abdul-Nour, G., Langheit, C., & Bourgeois, M. (2016). Risks of extreme and rare events in Asset Management. **Safety Science**, 88, 129-145.
- Korpela, K. (2015). Improving Cyber Security Awareness and Training Programs with Data Analytics. **Information Security Journal: A Global Perspective**, 24(1-3), 72–77.
- KPMG. (2018). **Building Cyber Resilience in Asset Management**. The Investment Association, May 2018.

- Kraemer, D. (2015). **Omni-Channel Logistics: A DHL perspective on implications**. DHL Customer Solution Innovation
- Krishnapriya , V., & Rupashree, B. (2014). Supply Chain Integration – A Competency based perspective. **International Journal of Managing Value and Supply Chains (IJMVSC)**, 5(3), 45.
- Kristof, K. (2016). **IRS Policies Protect 1.2 Million Identity Thieves**. [Retrieved March 04, 2020]. Available from: [http://www.cbsnews.com/8301-505144\\_162-36941966/irspolicies-protect-12-million-identity-thieves/](http://www.cbsnews.com/8301-505144_162-36941966/irspolicies-protect-12-million-identity-thieves/).
- Kumar, S.K., Tiwari, M.K., & Babiceanu R.F. (2010). Minimisation of supply chain cost with embedded risk using computational intelligence approaches. **International Journal of Production Research**, 48(13), 3717-3739.
- Kumar, S., & Sosnoski, M. (2011). Decision framework for the analysis and selection of appropriate transfer pricing for a resilient global SME manufacturing operation – a business case. **International Journal of Production Research**, 49(18), 5431-5448.
- Kumar, K., & Van Dissel, H. G. (1996). Sustainable Collaboration: Managing Conflict and Cooperation in Inter organizational Systems. **MIS Quarterly**, 279-300.
- Kumar, V., & Bhardwaj, A. (2018). Identity Management Systems: A Comparative Analysis. **International Journal of Strategic Decision Sciences**, 9(1), 63–78.
- Kwon, G., & Suh, T. (2004). Factors Affecting the Level of Trust and Commitment in Supply Chain Relationship. **Journal of Supply Chain Management**, 40(2), 4-14.
- Lamba, A., Singh, S., Balvinder, S., Dutta, N., & Rela, S. (2017). Analyzing And Fixing Cyber Security Threats For Supply Chain Management. **International Journal For Technological Research In Engineering**, 4(5).
- Lambert, D.M., Cooper, M.C., & Pagh, J.D. (1998). Supply chain management: implementation issues and research opportunities. **The International Journal of Logistics Management**, 9(2), 1-19.
- Landwehr, C.E. et al. (1994). A taxonomy of computer program security flaws. **ACM Computing Surveys**, 26(3), 211-254.
- Lankford, W.M. (2004). Supply chain management and the Internet. **Online Information Review Emerald Group Publishing Limited**, 28(4), 301-305.

- Laprie, J.C. (1985, June). Dependable computing and fault tolerance: concepts and terminology, **In 15<sup>th</sup> IEEE International Symposium on Fault-Tolerant Computing (FTCS-15)** (pp. 2 - 11). Michigan.
- Lee, J., and Lee, Y. (2016). A Holistic Model of Computer Abuse within Organizations. **Information Management and Computer Security**, 10(2/3), 57-63.
- Lee, J., Palekar, U. S., & Qualls, W. (2011). **Supply chain efficiency and security : Coordination for collaborative investment in technology**. European Journal of Operational Research, Vol. 210 No. 3, pp. 568–578.
- Lee, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2016). Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. **Journal of Computer Information Systems**, 57(4), 309–318.
- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. **European Journal of Information Systems**, 18, 177-187.
- Lengnick-Hall, C.A., & Beck, T.E. (2005). Adaptive fit versus robust transformation: how organizations respond to environmental change. **Journal of Management**, 31(5), 738-757.
- Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids - A comprehensive survey. **Computer Standards & Interfaces**, 56, 62–73.
- Levesque, P.J. (2012). Building resilience and sustainability into the Chinese supply chain. **Global Business and Organizational Excellence**, 31(3), 69-83.
- Levi, M. (2016). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. **Crime, Law and Social Change**, 67(1), 3–20.
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. **MIS Quarterly**, 33(1), 71-90.
- Liu Y., & Wang S. (2011). Research on Collaborative Management in Supply Chain Crisis. **Procedia Environmental Sciences**, 10, 141 – 146.
- Lockamy III, A., & McCormack, K. (2004a). The development of a supply chain management process maturity model using the concepts of business process orientation. **Supply Chain Management: An International Journal**, 9(4), 272-278.



- Lockamy III, A., & McCormack, K. (2004b). Linking SCOR planning practices to supply chain performance: An exploratory study. **International Journal of Operations & Production Management**, 24(12), 1192-1218.
- Luc, C. (2006). Collaboration planning in a supply chain. **Supply Chain Management: An International Journal**, 11(3), 249 – 258.
- Luca, U. (2009). Supply chain security - mitigation measures and a logistics multi-layered framework. **Journal of Transportation Security**, 3, 1-28.
- Luca, U., & Juha, H. (2017). Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement. **International Journal of Logistics Research and Applications**, 20(3), 276-295.
- Luiz, F.S., Paula, S.C., Silvio, P., & Katja, K. (2015). Supply Chain Resilience Analysis : A Brazilian Automotive Case. **RAE Sao Paulo**, 55(3), 304-313.
- Lynda, K., & Abdelhafid, Z. (2017). An Overview on Data Security in Cloud Computing. In **Proceedings of the Computational Methods in Systems and Software\_CoMeSySo 2017: Cybernetics Approaches in Intelligent Systems** (pp. 250-261).
- Macaulay, J., Buckalew, L. and Chung, G. (2015). Internet of Things in Logistics. **DHL Customer Solution Innovation**, 1–27.
- Magklaras GB, Furnell SM. (2012). **The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users**. [Retrieved March 05, 2020]. Available from: <http://folk.uio.no/georgios/papers/IWAR04MagklarasFurnell.pdf>.
- Machowiak, W. (2012). Risk management - unappreciated instrument of supply chain management strategy. **LogForum**, 8(4), 277-285.
- McCoy K. (2017). **Identity thieves tax the system**. [Retrieved March 06, 2020]. Available from: [http://www.usatoday.com/money/perfi/taxes/2008-04-10-id-theft\\_N.htm](http://www.usatoday.com/money/perfi/taxes/2008-04-10-id-theft_N.htm).
- McIlwraith, A. (2016). **Information security and employee behaviour: how to reduce risk through employee education, training and awareness**. Gower Publishing, Ltd..
- Madianou, M., Ong, J. C., Longboan, L., & Cornelio, J. S. (2016). The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery. **Journal of Communication**, 66(6), 960–981.

- Malatras, A., Coisel, I., & Sanchez, I. (2016, June). Technical recommendations for improving security of email communications. In **39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)**. MIPRO 2016, May 30 - June 3, 2016, Opatija, Croatia.
- Mandal, S. (2012), An empirical investigation into supply chain resilience. **IUP Journal of Supply Chain Management**, 9(4), 46-61.
- Mansour, A., Ahmad, A., Mohammad, M.H., Iehab, A.L.R., Zakirul, A.B. (2017). Improving risk assessment model of cyber security using fuzzy logic inference system. **Computers & Security**, 74, 323-339.
- Marco, F., & Paolo, T. (2016). Corporate sustainability approaches and governance mechanisms in sustainable supply chain management. **Journal of Cleaner Production**, 112(3), 1920-1933.
- Maria, B., Angela, M.S., & Jason, R.C.N. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In **International Conference on Cyber Security for Sustainable Society**, 2015.
- Marjorie, W. (2016). Objectives for managing cyber supply chain risk. **International Journal of Critical Infrastructure Protection**, 12, 4-11.
- Mark, W., & Joan, H. (2003). Building an Information Technology Security Awareness and Training Program. **Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)**, Oct 2003.
- Martin, G., Sandra, N. M., Marly, M. C., & Steve E. (2017). Business models and supply chains for the circular economy. **Journal of Cleaner Production**, 190, 712-721.
- Marwa, C., Mohamed, H., Sadok, E.A.(2017, January). A new architecture for supply chain management. In **14th IEEE Annual Consumer Communications & Networking Conference (CCNC)**, 8-11 Jan. 2017.
- Mavroeidis, V., & Bromander, S. (2017, September). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In **European Intelligence and Security Informatics Conference (EISIC)**. 11-13 Sept. 2017.

- Maylor, H., & Turner, N. (2017). Understand, reduce, respond: project complexity management theory and practice. **International Journal of Operations & Production Management**, 37(8), 1076-1093.
- McCormack, K., Bronzo Ladeira, M., & Paulo Valadares de Oliveira, M. (2008). Supply chain maturity and performance in Brazil. **Supply Chain Management: An International Journal**, 13(4), 272-282.
- Meepetchdee, Y., & Shah, N. (2007). Logistical network design with robustness and complexity considerations. **International Journal of Physical Distribution & Logistics Management**, 37(3), 201-222.
- Melad, M.A-D., Nurlida, B., & Madihah, M.S. (2017, July). Security Awareness Training: A Review. In **Proceedings of the World Congress on Engineering 2017 Vol I WCE 2017**, London, U.K.
- Melnyk, S.A., Davis, E.W., Spekman, R.E., & Sandor, J. (2010). Outcome-driven supply chains. **MIT Sloan Management Review**, 51(2), 32-38.
- Mehdi, K., Behrooz, D., & Abbas, R. (2017). Impact of Agility Capabilities in the Supply Chain Network. **International Journal of Scientific Study**, 5(3), 47-56.
- Michael, S., Chinedum, I., Harry, P., Devin, W., & Leah, K. (2018). **IT Asset Management Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)**. Nist Special Publication 1800-5, September 2018.
- Milan, P. (2012). Cyber Security Within The Globalization Process. **Journal of Defense Resources Management (JoDRM)**, 3(1), 19-26.
- Mohammaddust, F., Rezapour, S., Farahani, R. Z., Mofidfar, M., & Hill, A. (2017). Developing lean and responsive supply chains: A robust model for alternative risk mitigation strategies in supply chain designs. **International Journal of Production Economics**, 183, 632–653.
- Mohiuddin, A., Abdun, N. M., & Jiankun, H. (2016). A survey of network anomaly detection techniques. **Journal of Network and Computer Applications**, 60, 19-31.

- Nader, S.S. (2017). The information security landscape in the supply chain. **Computer Fraud & Security**, 2017(6), 16-20.
- Nader, S.S., Rossouw, V.S., & Steven, F.. (2016). Information security policy compliance model organizations. **Computers & Security**, 56, 70 - 82.
- Nagurney, A., Nagurney, & L.S., Shukla, S. (2015). A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability. **Cryptography, and Network Security**, 381-398.
- Narasimhan, R., Swink, M. & Kim, S.W. (2006). Disentangling leanness and agility: an empirical investigation. **Journal of Operations Management**, 24(5), 440-457.
- Neely, A., Gregory, M., & Platts, K. (1995). Performance measurement systems design: a literature review and research agenda. **International Journal of Operations & Production Management**, 15(4), 80-116.
- Neumann, P. G. (2016). Risks of Insiders. **Communications of the ACM**, 42(12), 160.
- Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. **Decision Support Systems**, 46(4), 815-825.
- Nieuwenhuis, L. J. M., Ehrenhard, M. L., & Prause, L. (2018). The shift to Cloud Computing: The impact of disruptive technology on the enterprise software business ecosystem. **Technological Forecasting and Social Change**, 129, 308–313.
- NIST. (2019). **The NIST Definition of Cloud Computing**, [Retrieved March 01, 2020]. Available from: <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>.
- Nyaga, G., Whipple, J., & Lynch, D. (2010). Examining supply chain relationships: do buyer and supplier perspectives on collaborative relationships differ?. **Journal of Operations Management**, 28(2), 101–114.
- Obeidat, M. A., and Turgay, T. (2013). Empirical Analysis for the Factors Affecting the Adoption of Cloud Computing Initiatives by Information Technology Executives. **Journal of Management Research**, 5(1), 152.
- Osaro, A., Zulkipli, G., & Radzuan, R. (2014). A Framework to Enhance Supply Chain Resilience: The Case of Malaysian Pharmaceutical Industry. **Global Business and Management Research: An International Journal**, 6(3), 219-228.

- Pahi, T., Leitner, M. and Skopik, F. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. In **Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)** (pp.334-345).
- Pahnilaa, S., Siponena, M., & Mahmoodb, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In **Proceedings of the 40th Hawaii International Conference on System Sciences**.
- Papastergiou, S., & Polemi, N. (2018). MITIGATE: A dynamic supply chain cyber risk assessment methodology. In **Smart Trends in Systems, Security and Sustainability** (pp. 1- 9). Springer, Singapore.
- Paul, A. G., Michael, E. G., James, L.F.. (2017). **NIST Special Publication 800-63-3 Digital Identity Guidelines**. National Institute of Standards and Technology. Available from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.
- Paul Ruggiero, J.F. (2017). **Cyber Threats to Mobile Phones**. [Retrieved March 20, 2020]. Available from : [https://www.uscert.gov/sites/default/files/publications/cyber\\_threats-to\\_mobilephones.pdf](https://www.uscert.gov/sites/default/files/publications/cyber_threats-to_mobilephones.pdf).
- Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. **International Journal of Logistics: Research and Applications**, 9(2), 127-142.
- Peck, H. (2005). Drivers of supply chain vulnerability: an integrated framework. **International Journal of Physical Distribution & Logistics Management**, 35(4), 210-232.
- Ponemon Institute. (2015). **Cost of Cyber Crime Study: United Kingdom**. [Retrieved March 04, 2020]. Available from: <http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports>.
- Pelgrin, W. (2014). A model for positive change: Influencing positive change in cyber security strategy, human factor, and leadership. **Information and Communication Security**, 107–117.
- Penthin S., Dillman R. (2015). **Digital SCM**. Available from [www.bearingpoint.com](http://www.bearingpoint.com), Germany.
- Pereira, J.V. (2009). The new supply chain's frontier: information management. **International Journal of Information Management**, 29(5), 372-379.

- Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. **Procedia Manufacturing**, 13, 1253-1260.
- Pettit, T.J., Fiksel, J., & Croxton, K.L. (2010). Ensuring supply chain resilience development of a conceptual framework. **Journal of Business Logistics**, 31(1), 1-21.
- Pettit, T.J., Croxton, K.L., & Fiksel, J. (2013). Ensuring supply chain resilience: development and implementation of an assessment tool. **Journal of Business Logistics**, 34(1), 46-76.
- Petit, F., & Lewis, L. P. (2017). Risk management and business continuity assessment: Importance of considering logical interdependencies. **Critical Infrastructure Protection Review**, 29, 29-35.
- Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path in a dynamic supply chain maritime risk management system. **Computer Standards & Interfaces**. 56, 74–82.
- Ponis, S.T., & Koronis, E. (2012). Supply chain resilience: definition of concept and its formative elements. **Journal of Applied Business Research**, 28(5), 921-930.
- Ponomarov, Y.S., & Holcomb, M.C. (2009). Understanding the concept of supply chain resilience. **The International Journal of Logistics Management**, 20(1), 124-143.
- Prakash J. Singh Damien Power. (2009). The nature and effectiveness of collaboration between firms, their customers and suppliers: a supply chain perspective. **Supply Chain Management: An International Journal**, 14(3), 189 – 200.
- Prakash, S., Soni, G. & Rathore, A. (2017). A critical analysis of supply chain risk management content: a structured literature review. **Journal of Advances in Management Research**, 14(1), 69-90.
- Presidential Policy Directive 21 (PPD-21). (2015). **Critical Infrastructure Security and Resilience”, U.S. Department of Homeland Security**. [Retrieved January, 2016]. Available From: <https://www.dhs.gov/what-security-and-resilience>.
- Qi, S., Zheng, Y., Li, M., Liu, Y., & Qiu, J. (2016). Scalable Industry Data Access Control in RFID-Enabled Supply Chain. **IEEE/ACM Transactions on Networking**, 24(6), 3551–3564.
- Qiang, Q., Anna, N., & June, D. (2009). Modeling of Supply Chain Risk Under Disruptions with Performance Measurement and Robustness Analysis, *Managing Supply Chain Risk and*

- Vulnerability: Tools and Methods for Supply Chain Decision Makers. In **Managing Supply Chain Risk and Vulnerability** (pp. 91-111). Springer, London.
- Qing, H., Robert, M., Sharon, W. & Pauline, F. (2015). Lean implementation within SMEs: a literature review. **Journal of Manufacturing Technology Management** , 26(7).
- Raab, M. and Griffin-Cryan, B. (2011). **Digital Transformation of Supply Chains: Creating Value—When Digital Meets Physical.**
- Rahim, N., Hamid, S., Mat Kiah, M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. **Kybernetes**, 44(4), 606-622.
- Raj, S. and Sharma, A. (2014). **Supply Chain Management in the Cloud.** Available from <https://www.accenture.com/tr-en/insight-supply-chain-management-cloud>.
- Rakesh, K.M., & Ravi, K. (2015). Green supply chain management (GSCM): a structured literature review and research implications. **Benchmarking: An International Journal**, 22(7).
- Ralston, P. (2014). **Supply chain collaboration: A literature review and empirical analysis to investigate uncertainty and collaborative benefits in regards to their practical impact on collaboration and performance.** Graduate Theses and Dissertations, Paper 13798.
- Ramaa, A., Rangaswamy, T.M., & Subramanya, K.N. (2009, December). A review of literature on performance measurement of supply chain network. In **2009 Second International Conference on Emerging Trends in Engineering & Technology** (pp. 802-807). IEEE.
- Ramanathan, U., Gunasekaran, A., & Subramanian, N. (2011). Supply chain collaboration performance metrics: a conceptual framework. **Benchmarking: An International Journal**, 18(6), 856-872.
- Ramuné, Č., & Milita, V. (2014). Agility and Responsiveness Managing Fashion Supply Chain. **Procedia - Social and Behavioral Sciences** , 150, 1012 – 1019.
- Randell B. (1975). System structure for software fault tolerance. **IEEE Transactions on Software Engineering**, SE-1(10), pp. 1220-232.

- Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. **Business Process Management Journal**, 18(3), 472-492.
- Reichhart, A. & Holweg, M. (2007). Lean distribution: concepts, contributions, conflicts. **International Journal of Production Research**, 45(16), 3699-3722.
- Rice, J.B., & Caniato, F. (2003). Building a secure and resilient supply network. **Supply Chain Management Review**, 7(5), 22-30.
- Richard, W. (2013). Supply Chain Template of the Resilience. **Operations Management**, 4, 8-12.
- Richter, K. and Poenicke, O. (2013). **Low-Cost Sensor Technology**.
- Roda, I., Parlikad, A. K., Macchi, M., & Garetti, M. (2016). A framework for implementing value-based approach in asset management. In **Proceedings of the 10th world congress on engineering asset management (WCEAM 2015)** (pp. 487-495). Springer, Cham.
- Rossouw, D. B., & SH V. S. (2016, May). Cybersecurity Governance: How can we measure it?. In **2016 IST-Africa Week Conference** (pp. 1-9). IEEE.
- Roumani, M. A., Fung, C. C., & Choejey, P. (2015, June). Assessing economic impact due to cyber attacks with System Dynamics approach. In **2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)** (pp. 1-6). IEEE.
- Rouse, M. (2016). **Digital Supply Chain, Search Manufacturing ERP.com**. [Retrieved March 03, 2020]. Available from: <http://searchmanufacturingerp.techtarget.com/definition/digital-supplychain?Vgnnextfmt=print>.
- Rusi, T., & Lehto, M. (2017). Cyber threats mega trends in cyber space. In **ICMLG 2017 5th International Conference on Management Leadership and Governance. Academic Conferences and Publishing Limited** (p. 323).
- Saeed, M. A., & Kersten, W.(2017). Supply chain sustainability performance indicators - a content analysis based on published standards and guidelines. **Logistic Research**, 10(12), 1-19.
- Saeed, M., & Kersten, W. (2019). Drivers of Sustainable Supply Chain Management: Identification and Classification. **Sustainability**, 11(4), 1137.



- Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. **European Journal of Operational Research**, 242(1), 261–273.
- Samaddar, S., & Kadiyala, S.S. (2006). An analysis of interorganisational resource sharing decisions in collaborative knowledge creation. **European Journal of Operational Research**, 170, 192–210.
- Sandor, B. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. **Technovation**, 34(7), 342-353.
- Sanislav, T., Mois, G., & Miclea, L. (2016). An approach to model dependability of cyber-physical systems. **Microprocessors and Microsystems**, 41, 67–76.
- Sarathy, R. (2006). Security and the global supply chain. **Transportation Journal**, 45(4), 28-51.
- Saridakis, G., Benson, V., Ezingard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. **Technological Forecasting and Social Change**, 102, 320–330.
- Saunders, W. S. A., & Becker, J. S. (2015). A discussion of resilience and sustainability: Land use planning recovery from the Canterbury earthquake sequence, New Zealand. **International Journal of Disaster Risk Reduction**, 14, 73–81.
- Samuel, W. (2016). **Factors Affecting Cyber Security In National Government Ministries In Kenya**. A Research Project of Master of Business Administration, Management of Information Systems, School of Business, University Of Nairobi October, 2016.
- Sawik, T. (2013). Selection of resilient supply portfolio under disruption risks. **Omega**, 41(2), 259-269.
- Schmitt, A.J., & Singh, M. (2012). A quantitative analysis of disruption risk in a multi-echelon supply chain. **International Journal of Production Economics**, 139(1), 22-32.
- Schmidt, B., Wallenburg, C.M., Rutkowsky, S., Einmahl, L., Petersen, I. and Klötzke, F. (2015) **Digital Supply Chains: Increasingly Critical for Competitive Edge**, (2015).
- Schumacker, R.E., & Lomax, R.G. (1996). **A beginner's guide to structural equation Modeling**. Mahwah, NJ: Lawrence Earlbaum.
- Scholten, K. & Schilder, S. (2015). The role of collaboration in supply chain resilience. **Supply Chain Management: An International Journal**, 20(4), 471 – 484.

- Schrauf, S. and Bertram, P. (2016). **Industry 4.0: How Digitization Makes the Supply Chain More Efficient, Agile, and Customer-focused, Strategy**. Available from: <http://www.strategyand.pwc.com/reports/industry4.0>.
- Sena, K. C., Melike, K., Huseyin, S. K., Sedef, K., & Ezgi, U. (2018). A Risk Assessment Model For Supply Chains. **PressAcademia Procedia (PAP)**, 7, 122-125.
- Serhiy, Y. P., & Mary, C. H. (2009). Understanding the concept of supply chain resilience. **The International Journal of Logistics Management**, 20(1), 124 – 143.
- Setiawan, A., Wibowo, A., & Susilo, A. H. (2017). Risk analysis on the development of a business continuity plan. In **2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)** (pp. 1-4). IEEE.
- Shaghayegh, M.A.R., Seyedeh, K. T., Syed, A.R. & Saif Ur, R.K. (2014). Organizational Culture, IT Competence, and Supply Chain Agility in Small and Medium-Size Enterprises. **Global Business and Organizational Excellence**, 33(6), 69-75.
- Shakarian, P., Shakarian, J., & Ruef, A. (2013). **Introduction to Cyber-Warfare: A Multidisciplinary Approach**. Waltham, MA: Elsevier.
- Sharma, V., Dixit, A. R., & Qadri, M. A. (2015). Impact of lean practices on performance measures in context to Indian machine tool industry. **Journal of Manufacturing Technology Management**. 26(8).
- Shepherd, C. & Gunter, H. (2006). Measuring supply chain performance: current research and future directions. **International Journal of Productivity and Performance Management**, 55(3/4), 242-258.
- Sheffi, Y. (2005). Preparing for the big one. **IEE Manufacturing Engineer**, 84(5), pp. 12-15.
- Sheffi, Y., & Rice, J.B. (2005). A supply chain view of the resilient enterprise. **MIT Sloan Management Review**, 47(1), 41-48.
- Shatat, A.S., & Udin, Z.M. (2012). The relationship between ERP system and supply chain management performance in Malaysian manufacturing companies. **Journal of Enterprise Information Management**, 25(6), 576 – 604.
- Shi, M., & Yu, W. (2013). Supply chain management and financial performance: literature review and future directions. **International Journal of Operations & Production Management**, 33(10), 1283 – 1317.

- Shore, B. (2001). Information sharing in global supply chain systems. **Journal of Global Information Technology Management**, 4(3), 27-50.
- Simatupang, T. M., Wright, A. C., & Sridharan, R. (2004). Applying theory of constraints to supply chain collaboration. **Supply chain Management: an international journal**, 9(1), 57-70.
- Simatupang, T. M., & Sridharan, R. (2002). The collaborative supply chain. **International Journal of logistics management**, 13(1), 15-30.
- Simatupang T. M., & Sridharan, R. (2008). Design for supply chain Collaboration. **Business Process Management Journal**, 14(3), 401-418.
- Sirirat, S., Mathupayas, T., & Atcharawan, N. (2015). Factors Affecting Computer Crime Protection Behavior. In **PACIS 2015** (p. 31).
- Spiegler, V.L., Mohamed, M.N., & Wikner, J. (2012). A control engineering approach to the assessment of supply chain resilience. **International Journal of Production Research**, 50(21), 6162-6187.
- Stewart, G.T., Kolluru, R., & Smith, M. (2009). Leveraging public-private partnerships to improve community resilience in times of disaster. **International Journal of Physical Distribution & Logistics Management**, 39(5), 343-364.
- Shukla, A., Lalit, V.A., & Venkatasubramanian, V. (2011). Optimizing efficiency-robustness trade-offs in supply chain design under uncertainty due to disruptions. **International Journal of Physical Distribution & Logistics Management**, 41(6), 623-647.
- Somuyiwa, A. O., Adebayo, I. T., & Akanbi, T. A. (2011). Supply Chain Performance: An Agile Supply Chain Driven By Information System (Is) Capabilities. **British Journal of Arts and Social Sciences** , 1(2), 125-135.
- Spyridon, P., Nineta, P. (2017). MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology. In **Smart Trends in Systems, Security and Sustainability** (pp.1-9). Springer, Singapore.
- Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behavior. . In **PACIS 2015** (p. 31).
- Stavros T. P., & Athanasia, C. N.. (2016). Supply Chain Risk Management Frameworks and Models: A Review. **International Journal of Supply Chain Management**, 5(4), 1-11.

- Stewardship Economics Group. (2016). **Cloud Computing and SME's in UK**. A report from the Cloud Stewardship Economics Project Group sponsored by Technology Strategy Board; Available from: [http://www.iisp.org/imis15/Cloud\\_Computing\\_and\\_SME's\\_in\\_UK.pdf](http://www.iisp.org/imis15/Cloud_Computing_and_SME's_in_UK.pdf).
- Stoicescu, M., Fabre, J.-C., & Roy, M. (2017). Architecting resilient computing systems: A component-based approach for adaptive fault tolerance. **Journal of Systems Architecture**, 73, 6–16.
- Strohmeier, M., Schafer, M., Pinheiro, R., Lenders, V., & Martinovic, I. (2016). On Perception and Reality in Wireless Air Traffic Communication Security. **IEEE Transactions on Intelligent Transportation Systems**, 18(6), 1338-1357.
- Sujit, R.C., Sina, F., Nafiul, R., & Mohammad, A.A.F. (2017). Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. **Journal of Hardware and Systems Security**, 2(1), 51-68.
- Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. **International Journal of Distributed Sensor Networks**, 10, 1-9.
- Supply Chain Council. (2005). **Supply Chain Operations Reference (SCOR) model: overview -version 10.0**. available from: <http://supply-chain.org/f/SCOR-Overview-Web.pdf>
- Swafford, P.M., Ghosh, S., & Murthy, N. (2006). The antecedents of supply chain agility of a firm: scale development and model testing. **Journal of Operations Management**, 24(2), 170-188.
- Synmatec. (2014). **The Cyber Resilience Blueprint: A New Perspective on Security**. Synmatec Cooperation.
- Tadas, L., Tomas, P., Konstantin, A., & Martynas, D. (2017). Cyber Security Management Model For Critical Infrastructure. **The International Journal Entrepreneurship And Sustainability Issues**, 4(4), 559-573.
- Tarn, J. M., Yen, D.C., & Beaumont, M. (2002). Exploring the rationales for ERP and SCM integration. **Industrial Management & Data Systems**, 102(1), 26 – 34.
- TechTalkThai. **Cyber Resilience แนวคิดสำหรับรับมือกับ Unknown Threats**. [Retrieved March 5, 2016]. Available from: <https://www.techtalkthai.com/cyber-resilience-and-unknown-threats/>.

- The Australian Securities & Investments Commission (ASIC). (2015). **Haven't Carried Out a Cyber Resilience 'Health Check'? You Could be in Breach of Regulations.** [Retrieved January, 2016]. Available from: <https://www.criterionconferences.com/blog/government/havent-carried-cyber-resilience-health-check-breach-regulations/>.
- The Digital Supply Chain Initiative. (2015). **Digital Supply Chains: A Frontsite Flip.** Sanya, China.
- The Information Security Forum, ISF. (2016). **Threat Horizon 2016– On The Edge of Trust: Executive Summary.** Threat Horizon 2016.
- Thomas, R., & Buchanan, B. (2014). Attributing Cyber Attacks. **Journal of Strategic Studies**, 38(1-2), 4–37.
- Thomsett, M.C. (2011). Global supply chain risk management: viewing the past to manage today's risks from an historical perspective. **Review of Management Innovation & Creativity**, 4(9), 44-54.
- Timothy, J. P., Keely L. C., & Joseph F. (2013). Ensuring Supply Chain Resilience: Development and Implementation of an Assessment Tool. **Journal of Business Logistics**, 34(1), 46–76.
- Tiwari, S., Wee, H.M. and Daryanto, Y. (2018). Big data analytics in supply chain management between 2010 and 2016: Insights to industries. **Computer Industrial Engineer**, 115, 319–330.
- Tobiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T., & Yagi, T. (2016, June). Malware Detection with Deep Neural Network Using Process Behavior. In **2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)** (Vol. 2, pp. 577-582). IEEE.
- Toka, A., Aivazidou, E., Antoniou, A., & Arvanitopoulos-Darginis, K. (2013). Cloud Computing in Supply Chain Management: An Overview. In **E-logistics and e-supply chain management: applications for evolving business** (pp. 218-231). IGI Global.
- Watchguard (2015). **Top 10 Threats to SME Data Security.** [Retrieved March 03, 2020] Available from: [https://www.watch-guard.com/docs/whitepaper/wg\\_top10-summary\\_wp.pdf](https://www.watch-guard.com/docs/whitepaper/wg_top10-summary_wp.pdf).

- Torres J.R.M., Vargas D.A.O. (2013). Collaboration and information sharing in dyadic supply chains: A literature review over the period 2000–2012. **Estudios Gerenciales**, 30, 343-354.
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. **Computers & Security**, 72, 212–233.
- Tracey, S., O’Sullivan, T. L., Lane, D. E., Guy, E., & Courtemanche, J. (2017). Promoting Resilience Using an Asset-Based Approach to Business Continuity Planning. **SAGE Open**, 7(2), 1-15.
- TrendMicro, (2015). **Bad Ads and Zero-Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices**. TrendLabs 1Q 2015 Security Roundup, 2015.
- Tsuchiya, A., Fraile, F., Koshijima, I., Órtiz, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. **Journal of Industrial Engineering and Management (JIEM)**, 11(2), 318 - 333.
- Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of Risk Management Implementation for Industry 4.0. **Procedia Manufacturing**, 11, 1223-1230.
- Urciuoli, L. (2013). Cyber resilience: A strategic approach for supply chain management. **Technology Innovation Management Review**, 5(4).
- Vachon, S., Robert, D.K. (2007). Environmental management and manufacturing performance : The role of collaboration in the supply chain. **International Journal of Production Economics**, 111, 299–315.
- Valikangas, L. (2010). **The Resilient Organization: How Adaptive Cultures Thrive Even When Strategy Fails**. McGraw-Hill, New York, NY.
- Varshney, G., & Gupta, H. (2017). A security framework for IOT devices against wireless threats. In **2017 2nd International Conference on Telecommunication and Networks TEL- NET** (p. 1-6). IEEE.
- Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. **Information and Software Technology**, 94, 30 -37.
- Verbano, C., & Venturini, K. (2011). Development paths of risk management: approaches, methods and fields of application. **Journal of Risk Research**, 14(5), 519-550.

- Verizon. (2014). **Data Breach Investigations Report**. [Retrieved March 03,2020]. Available from <http://www.verizonenterprise.com/DBIR/2014/#sthash.x7SaQWVv.dpuf.pdf>
- Vlajic, J. V. (2015). Vulnerability and robustness of SME supply chains: An empirical study of risk and disturbance management of fresh food processors in a developing market. In **R. Bhamra (Ed.), Organisational Resilience: Concepts, Integration, and Practice** (pp. 85-102). CRC press, Taylor and Francis.
- Voss, M.D., Whipple J.M., & Closs, D.J. (2009). The role of strategic security: internal and external security measures with security performance implications. **Transportation Journal**, 48(2), 5-23.
- Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. **Security and Communication Networks**. 2018.
- Wakolbinger, T. & Cruzb J.M. (2011). Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts. **International Journal of Production Research**, 49(13), 4063–4084.
- Wallace, S.W., & Choi, T.M. (2011). Flexibility, information structure, options, and market power in robust supply chains. **International Journal of Production Economics**, 134(2), 284-288.
- Walden E. A., (2015). Intellectual property rights and cannibalization in information technology outsourcing contracts. **MIS Quarterly**, 134 (2), 284-288.
- Waleed, A-G. (2016). Extending Protection Motivation Theory to Understand Security Determinants of Anti-virus Software Usage on Mobiles Devices. **International Journal Of Computers**,10(2016), 125-138.
- Walter, A. (2003). Relationship-specific factors influencing supplier involvement in customer new product development. **Journal of Business Research**, 56(9), 721–733.
- Wang, G., Gunasekaran, A. Ngai, E.W.T., and Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management: certain investigations for research and applications, **International Journal Production Economics**, 176, 98–110.
- Warren, M. & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: a short note. **International Journal of Physical Distribution & Logistics Management**, 30(7/8), 710 -716.

- Wieland, A., & Wallenburg, C.M. (2012). Dealing with supply chain risks: linking risk management practices and strategies to performance. **International Journal of Physical Distribution & Logistics Management**, 42(10), 887-905.
- Wieland, A. (2013). Selecting the right supply chain based on risks. **Journal of Manufacturing Technology Management**, 24(5), 652-668.
- Wieland, A. & Wallenburg, C.M. (2013). The influence of relational competencies on supply chain resilience: a relational view. **International Journal of Physical Distribution & Logistics Management**, 43(4), 300 – 320.
- Wildgoose, N., Brennan, P. & Thompson, S. (2012). Understanding your supply chain to reduce the risk of supply chain disruption. **Journal of Business Continuity & Emergency Planning**, 6(1), 5-67.
- Williams, Z., Ponder, N., & Autry, C.W. (2009), Supply chain security culture: measure development and validation. **The International Journal of Logistics Management**, 20(20), 243-260.
- Windelberg, M. (2016). Objectives for managing cyber supply chain risk. **International Journal of Critical Infrastructure Protection**, 12, 4–11.
- Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In **Proceedings of ICIS 2005** (pp. 31).
- Womack, J., Jones, D., & Roos, D. (1990). **The machine that changed the world**. New York: Harper Perennial.
- Womack, J. P.; Jones, D. T. & Roos, D. (1991). **The Machine That Changed the World : The Story of Lean Production**. Harper Perennial.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. **Computers in Human Behavior**, 24(6), 2799-2816.
- Wu, T., Huang S.M., Blackhurst, J., Zhang, X.L. & Wang, S.S. (2013). Supply chain risk management: an agent-based simulation to study the impact of retail stockouts. **IEEE Transactions on Engineering Management**, 60(4), 676-686.



- Xiao, R., Tongyang, Y., & Gong, X. (2012). Modeling and simulation of ant colony's labor division with constraints for task allocation of resilient supply chains. **International Journal on Artificial Intelligence Tools**, 21(3), 1-19.
- Xu, J. (2014). **Managing Digital Enterprise**. Atlantis Press, Paris.
- Yadav, S. A., Kumar, S. R., Sharma, S., & Singh, A. (2016). A review of possibilities and solutions of cyber attacks in smart grids. In **2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)** (pp. 60-63). IEEE.
- Yang, Z., Aydin, G., Babich, V., & Beil, D.R. (2009). Supply disruptions, asymmetric information, and a backup production option. **Management Science**, 55(2), 192-209.
- Yang, B., & Yang Y. (2010). Postponement in supply chain risk management: a complexity perspective. **International Journal of Production Research**, 48(7), 1901-1912.
- Yang, C.-L., Huang, C.-Y., Kao, Y.-S., & Tasi, Y.-L. (2017). Disaster Recovery Site Evaluations and Selections for Information Systems of Academic Big Data. **Eurasia Journal of Mathematics, Science and Technology Education**, 13(8), 4553 – 4589.
- Yan, H., Lou, S., & Sethi, S.P. (2000). Robustness of various production control policies in semiconductor manufacturing. **Production and Operations Management**, 9(2), 171-183.
- Yamane, T. (1973). **Statistics: An Introductory Analysis (3rd ed)**. USA: Harper & Row.
- Zailani, S., Seva Subaramaniam, K., Iranmanesh, M., & Shaharudin, M. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator. **International Journal of Physical Distribution & Logistics Management**, 45(7), 652-673.
- Zeng, Z., & Zio, E. (2017). An integrated modeling framework for quantitative business continuity assessment. **Process Safety and Environmental Protection**, 106, 76–88.
- Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. **Information Management & Computer Security**, 17(4), 330 - 340.

- Zhengan, H., Shengli, L., Xianping, M., Kefei, C., & Jin, L. (2017). Insight of the protection for data security under selective opening attacks. **Information Sciences**, 412, 223 - 241.
- Zobel, C.W. & Khansa, L. (2012). Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks. **Decision Sciences**, 43(4), 687-710.
- Zsidisin, G.A., & Wagner, S.M. (2010). Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence. **Journal of Business Logistics**, 31(2), 1-20.