BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Serangan *cyber* merupakan phenomena dengan tingkat perkembangan yang mengikuti pertumbuhan dan perkembangan teknologi. Kemampuan dari serangan *cyber* berorientasi terhadap tiga hal, yaitu (1) manipulasi data, (2) pencurian data dan (3) menghilangkan aksesbilitas dari suatu sistem dalam rangka pengguna lainnya tidak mengakses sistem tersebut. Secara umum serangan *cyber* diklasifikasi menjadi dua kategori, yaitu (1) penyerangan terhadap suatu sistem, perangkat lunak atau perangkat keras dan (2) penyerangan terhadap individu atau pengguna dari suatu sistem; dimana, serangan tersebut berorientasi atas tiga konsep utama dalam keamanan informasi dan teknologi yaitu terkait sisi *confidentiality*, *integrity* dan *availability* dari suatu sistem maupun data digital. Sehingga, hal tersebut mendorong setiap perusahaan atau organisasi yang menggunakan sistem keamanan terhadap data dan teknologi yang digunakan untuk mempunyai pendekatan dan sistem keamanan yang memadai untuk memitigasi risiko dan dampak yang dapat ditimbulkan dari serangan *cyber*.

Berdasarkan hal tersebut, dalam rangka menjawab pertanyaan penelitian dan memenuhi tujuan penelitian yang telah ditentukan, maka metode yang digunakan dalam rangka mengidentikasi setiap sumber pemicu yang dapat menimbulkan serangan *cyber* pada perusahaan fintech X ialah dengan menggunakan metode *fault tree analysis* (FTA). Serta, terkait menemukan nilai estimasi kerugian secara finansial untuk setiap insiden yang terjadi metode *single loss expectancy* (SLE) diterapkan dan metode *annualized loss expectancy* (ALE) diterapkan untuk menemukan nilai estimasi kerugian finansial yang dapat terjadi dalam kurun waktu tahunan pada perusahaan fintech X.

Terkait pertanyaan mayor yang harus dijawab pada penelitian ini terhadap sumber pemicu yang dapat menimbulkan serangan *cyber* pada perusahaan fintech X, ditemukan bahwa ketiadaan *early-warning system*, pencatatan sistem yang tidak akurat dan tidak adanya *system pattern analyzer* dalam rangka mendeteksi perilaku yang mencurigakan dari pengguna aplikasi memicu terjadinya insiden penyalahgunaan akun. Sedangkan ketidaktahuan pengguna dan penggunaan identitas personel perusahaan memicu terjadinya inisiden modus penipuan dengan jenis *social engineering*.

Terhadap kerugian finansial dan nilai estimasi dari sumber pemicu yang menghasilkan insiden penyalahgunaan akun, ditemukan bahwa kerugian yang telah terjadi telah mencapai Rp. 33 juta; terkait estimasi kerugian finansial dari insiden penyalahgunaan akun, diestimasikan nilai kerugian finansial mencapai Rp. 4.76 juta per insiden, sementara nilai estimasi kerugian finansial dalam kurun waktu tahunan mencapai Rp. 5.5 juta per tahun. Sedangkan terhadap insiden modus penipuan dengan jenis *social engineering*, kerugian finansial yang telah terjadi mencapai Rp. 9 juta; terkait nilai estimasi kerugian finansial, diestimasikan bahwa sumber pemicu yang menimbulkan insiden modus penipuan mencapai Rp. 9 juta per insiden, sedangkan nilai estimasi kerugian finansial dalam kurun waktu tahunan mencapai Rp. 1.5 juta.

Terkait nilai frekuensi dan probabilitas atas sumber pemicu yang menghasilkan insiden penyalahgunaan akun, ditemukan bahwa probabilitas atas insiden tersebut mencapai nilai 1.167 dengan frekuensi atas insiden tersebut telah terjadi sebanyak tujuh kali dalam kurun waktu enam tahun. Sedangkan terhadap insiden modus penipuan dengan jenis *social engineering*, frekuensi atas insiden tersebut telah terjadi sebanyak satu kali dalam enam tahun; dengan nilai probabilitas atas insiden tersebut mencapai nilai 0.167.

Terhadap insiden yang telah terjadi pada perusahaan fintech X, perusahaan fintech X telah mengambil tindakan pemblokiran perangkat keras dan melakukan blacklist terhadap individu yang telah menyalahgunakan aplikasi dari perusahaan fintech X. Sedangkan terhadap insiden modus penipuan dengan jenis *social engineering*, perusahaan fintech X telah melakukan kegiatan sosialiasi kepada

pengguna dalam menjaga akun yang dimiliki dari modus penipuan dan telah melakukan proses investigasi atas insiden modus penipuan yang telah terjadi kepada para pengguna.

Terkait performa perusahaan dalam mengimplementasikan konsep manajemen risiko dalam menghadapi serangan *cyber* terhadap sistem keamanan IT yang dimiliki, ditemukan bahwa tindakan penanggulangan atas insiden yang telah terjadi dilakukan secara langsung namun tidak dilakukan pencatatan atau dokumentasi atas insiden dan tindakan yang diterapkan dalam menyelesaikan masalah tersebut. Walaupun perusahaan fintech X mempunyai kapabilitas dalam mereduksi dampak yang ditimbulkan dari suatu insiden, namum secara jangka panjang perusahaan fintech X berpotensi untuk membutuhkan waktu lama dalam menyelesaikan suatu risiko atau masalah yang sering terjadi.

Terkait pengembangan protokol keamanan yang digunakan untuk menindak lanjuti tindakan yang telah diterapkan oleh perusahaan fintech X untuk memitigasi dan mereduksi dampak dari insiden yang telah terjadi, penerapan sistem berbasis *big data* dapat diterapkan untuk menganalisa aktivitas dari akun para pengguna (baik pergerakan saldo uang elektronik dan perilaku para pengguna akun) dan melakukan pembaharuan data terhadap individu yang telah di *blacklist* untuk mencegah individu tersebut untuk menggunakan kembali aplikasi yang dihasilkan oleh perusahaan fintech X. Sedangkan terhadap pengembangan protokol keamanan dalam menghadapi modus penipuan dengan jenis *social engineering*, perusahaan fintech X dapat menerapkan konsep *customer due diligence* terhadap aplikasi yang digunakan oleh para pengguna, memastikan aplikasi tersebut untuk tidak dapat mengakses situs diluar domain sistem perusahaan fintech X dan melakukan perubahan *one-time password* secara berkala, terutama terhadap fitur transfer dan pembayaran.

Terakhir, terkait temuan yang telah diperoleh pada perusahaan fintech X, ditemukan bahwa perusahaan fintech X tidak memenuhi tujuan dari bagian 16.1 annex A yang tertulis pada standard ISO/IEC 27001:2013 dikarenakan perusahaan fintech X tidak secara konsisten melakukan pencatatan atau dokumentasi terhadap insiden yang berorientasi terhadap keamanan informasi dan teknologi.

Dokumentasi yang tidak konsisten tidak hanya terjadi pada insiden yan telah terjadi melainkan terhadap aset yang dimiliki oleh perusahaan fintech X, sehingga perusahaan fintech X tidak memenuhi bagian A.8 terkait pendataan aset yang digunakan pada sistem keamanan informasi dan teknologi perusahaan.

Berdasarkan penelitian yang telah dilakukan, penelitian ini mempunyai implikasi terhadap perusahaan atau organisasi yang menggunakan sistem keamanan dalam melindungi informasi dan teknologi yang dimiliki dalam menjalankan kegiatan bisnis yang dilakukan dari serangan *cyber*. Penentuan kebijakan atau tindakan yang dapat diterapkan perusahaan dalam memitigasi dan mereduksi dampak dari risiko yang ditimbulkan dari serangan *cyber* menentukan kapabilitas perusahaan dalam melindungi data yang dimiliki, dimana serangan *cyber* yang dapat berasal dari sisi internal atau eksternal perusahaan. Apabila perusahaan tidak dapat menentukan tindakan dan kesimpulan dari tren serangan *cyber* yang terjadi maka perusahaan tersebut berpotensi untuk mengalami kerugian secara finansial dan non-finansial.

5.2 Saran

Berdasarkan penelitian, temuan dan analisis yang telah dilakukan terhadap penerapan manajemen risiko terhadap keamanan informasi dan teknologi pada perusahaan fintech (secara khusus terhadap perusahaan fintech X), terdapat empat saran atau rekomendasi yang dapat diterapkan dalam rangka meningkatkan performa perusahaan dalam memitigasi dan mereduksi dampak yang disebabkan oleh serangan *cyber*; serta dalam melakukan pendataan atau dokumentasi yang dapat mempermudah perusahaan dalam menganalisa insiden atau risiko yang berorientasi terhadap keamanan informasi dan teknologi. Diberikan sebagai berikut:

Pertama, berkaitan dengan temuan terhadap pencatatan atau dokumentasi insiden, disarankan untuk setiap perusahaan atau organisasi yang menggunakan sistem informasi dan teknologi untuk menetapkan standard atau format pencatatan atau dokumentasi terhadap insiden yang telah terjadi; terutama terhadap insiden atau masalah yang berorientasi terhadap serangan *cyber* dan telah menimbulkan

kerugian secara masif. Hal tersebut disarankan untuk dilakukan dalam rangka untuk menemukan pola atau karakteristik dari insiden atau masalah yang telah terjadi. Serta, hal tersebut dapat memberikan kapabilitas kepada perusahaan dalam menghasilkan dan menentukan keputusan, kesimpulan dan prioritas yang sesuai dengan insiden dan risiko yang dihadapi. Format saran terhadap pencatatan suatu insiden dan risiko disertakan pada Lampiran 3. Secara sederhana, dengan menerapkan format pencatatan yang disertakan pada Lampiran 3, maka perusahaan fintech X mempunyai kapabilitas dalam memetakan karakteristik dari serangan *cyber* terkait objek dengan tingkat frekuensi tertinggi dari serangan *cyber*, rata-rata kerugian yang ditimbulkan dari suatu insiden, pendekatan yang digunakan oleh para *hacker* dalam menjalankan serangan *cyber* dan sumber pemicu utama yang dapat menimbulkan insiden tersebut. Dimana, informasi tersebut dapat digunakan oleh perusahaan fintech X dalam menghasilkan kebijakan atau tindakan yang dapat memitigasi terjadinya insiden dan dampak yang ditimbulkan dari insiden yang berorientasi terhadap keamanan informasi dan teknologi

Kedua, terkait indikasi ketidakseragaman informasi atau *information asymmetry* pada struktur organisasi perusahaan, disarankan untuk menentukan pegawai yang memiliki tugas dalam melakukan pencatatan atau dokumentasi terhadap insiden yang telah terjadi dan menentukan tempat untuk para pegawai untuk melaporkan insiden yang muncul pada perusahaan (*single point of contact*). Baik secara pencatatan secara sistem (*system logging*) atau pencatatan secara manual. Serta membuat pegawai tersebut bertanggung jawab dalam memastikan para pemegang keputusan perusahaan dan departemen manajemen risiko untuk mempunyai pemahaman atau informasi yang sama terhadap insiden atau risiko yang dihadapi oleh perusahaan. Hal tersebut disarankan untuk dilakukan dalam rangka untuk memberikan kapabilitas kepada perusahaan untuk dapat menentukan prioritas terhadap insiden atau risiko yang dapat ditangani, dimitigasi atau diselesaikan; terutama terhadap insiden atau risiko yang mempunyai dampak dalam skala masif dan destruktif kepada perusahaan.

Ketiga, terkait durasi waktu penyimpanan data transaksi yang dilakukan oleh para pengguna, perusahaan disarankan untuk menambah kapasitas media

penyimpanan digital terhadap perangkat keras yang dimiliki. Hal tersebut disarankan untuk diterapkan dalam rangka untuk memberikan kapabilitas kepada perusahaan dalam melakukan pembacaan pola secara ekstensif terhadap perubahan atau pergerakan nilai saldo uang elektronik yang dimiliki oleh para pengguna. Dimana, hal tersebut dapat membantu perusahaan dalam mendeteksi perubahan atau pergerakan nilai uang elektronik yang mencurigakan atau pergerakan uang elektronik yang pada umum berada diluar kebiasaan para pengguna.

Keempat, terkait mendeteksi perilaku para pengguna dalam menggunakan aplikasi, perusahaan yang menggunakan sistem informasi dan teknologi disarankan untuk menerapkan sistem berbasis *big data* dalam membaca perilaku para pengguna aplikasi. Hal tersebut disarankan untuk diterapkan dalam rangka untuk memberikan kapabilitas kepada perusahaan dalam mendeteksi perilaku yang berpotensi untuk menimbulkan kerugian secara finansial dan non-finansial baik kepada perusahaan maupun para pengguna. Dimana, hal tersebut dapat membantu perusahaan dalam menandai perilaku yang mencurigakan atau diluar kebiasaan yang sebelumnnya tidak terdeteksi dari pembacaan pola yang berfokus terhadap pergerakan saldo uang elektronik yang dimiliki oleh para pengguna.

Kelima, Dalam rangka meningkatkan performa perusahaan fintech X dalam mengimplementasikan konsep manajemen risiko terhadap keamanan informasi dan teknologi berdasarkan standard ISO/IEC 27001:2013 maka perusahaan fintech X disarankan untuk terlebih dahulu melakukan pencatatan secara intensif terkait insiden yang telah terjadi, terutama terhadap insiden yang berorientasi terhadap keamanan informasi dan data pengguna maupun perusahaan. Hal tersebut disarankan untuk dilakukan dalam rangka perusahaan fintech X mempunyai kapabilitas untuk memetakan objek utama terjadinya serangan *cyber* dan pendekatan yang digunakan oleh para *hacker* dalam melakukan serangan *cyber*. Serta, dengan informasi tersebut perusahaan fintech X mempunyai kapabilitas dalam menghasilkan kebijakan atau tindakan yang dapat meningkatkan kualitas penjagaan informasi dan data pengguna maupun perusahaan dari serangan *cyber*. Terutama terhadap insiden serangan *cyber* yang ditujukan kepada para pengguna aplikasi dengan jenis *social engineering*.

Keenam, terkait insiden terhadap penyalahgunaan akun dan modus penipuan dengan jenis *social engineering* yang telah terjadi pada perusahaan fintech X, disarankan perusahaan menerapkan konsep *customer due diligence* dan *know your customer* (KYC) dalam rangka memperoleh pola penggunaan aplikasi dari para pengguna, dan data tersebut dapat digunakan kepada sistem yang dimiliki untuk mendeteksi perilaku yang mencurigakan atau diluar kebiasaan dalam menggunakan aplikasi dalam rangka melindungi pengguna maupun perusahaan terhadap perilaku yang berpotensi untuk menimbulkan kerugian finansial dan non-finansial.

Berdasarkan saran yang telah diberikan terhadap perusahaan yang menggunakan sistem informasi dan teknologi (terutama perusahaan fintech X), dapat disimpulkan bahwa performa terhadap penerapan manajemen risiko terhadap keamanan informasi dan teknologi dapat dikembangkan apabila perusahaan tersebut mempunyai fondasi terhadap konsep keamanan informasi dan teknologi yang telah diterima, diadopsi dan menjadi bagian dari kultur perusahaan.

DAFTAR REFERENSI

Affia, A.-A. O. (2018). *Security Risk Management of E-commerce Systems*. Master's thesis, University of Tartu.

Anandan, R., Sipahimalani, R., Saini, S., Aryasomayajula, S., & Smittinet, W. (2018). *e-Conomy SEA 2018: Southeast Asia's internet economy hits an inflection point*. Mountain View: Google LLC. Source: https://www.thinkwithgoogle.com/_qs/documents/6870/Report_e-Conomy_SEA_2018_by_Google_Temasek_121418_cpsLjlQ.pdf.

Aven, T. (2015). *Risk Analysis*. Chichester: John Wiley & Sons, 2nd edition.

Bank Indonesia (2018). *Peraturan Bank Indonesia Nomor 20/6/PBI/2018 Tentang Uang Elektronik*. Peraturan Bank Indonesia No. 20/6/PBI/2018, Bank Indonesia (BI), Jakarta.

Baur, C. & Wee, D. (2015). Manufacturing's Next Act. Retrieved from McKinsey & Company: http://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act.

Bendovschi, A. (2015). Cyber-Attacks - Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24–31.

Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. Working Paper WP/18/143, International Monetary Fund (IMF), Washington DC.

Callen-Naviglia, J. & James, J. (2018). FinTech, RegTech and The Importance of Cybersecurity. *Issue in Information Systems*, 19(3), 220–225.

Chapman, R. J. (2011). *Simple Tools and Techniques for Enterprise Risk Management*. Chichester: John Wiley & Sons, 2nd edition.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *CISSP Certified Information Systems Security Professional - Offical Study Guide*. Indianapolis: John Wiley & Sons, 8th edition.

Check Point Research (2018). *2018 Security Report: Welcome To The Future of Cyber Security*. Security Report, Check Point Software Technologies LTD.

Cisco (2018a). *Annual Cybersecurity Report 2018*. Cybersecurity Report, Cisco Systems Inc. Source: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

Cisco (2018b). *Asia Pasific Security Capabilities Benchmark Study: Regional Breaches Readiness*. Cisco 2018 Annual Cybersecurity Report, Cisco Systems Inc. Source: https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf.

Dapp, T. F. & Slomka, L. (2014). *Fintech – The digital (r)evolution in the financial sector.* Research Report, Deutsche Bank.

Dapp, T. F. & Slomka, L. (2015). *Fintech reloaded – Traditional banks as digital ecosystems*. Research Report, Deutsche Bank.

Databoks.co.id (2018). T-cash, Aplikasi Uang Elektronik Paling Banyak Dipakai di Indonesia. Retrieved from Katadata.co.id: https://databoks.katadata.co.id/datapublish/2018/02/06/siapa-pemain-uang-elektronik-berbasis-aplikasi.

Databoks.co.id (2019). Transaksi Gopay Mencapai Rp. 89 Triliun. Retrieved from Katadata.co.id: https://databoks.katadata.co.id/datapublish/2019/03/01/transaksi-gopay-mencapai-rp-89-triliun.

Davis, K., Maddock, R., & Foo, M. (2017). Catching up with indonesia's fintech industry. *Law and Financial Markets Review*.

Depository Trust & Clearing Corporation (2017). *Systemic Risk Barometer*. Systemic Risk Report, Depository Trust & Clearing Corporation (DTCC), New York.

Depository Trust & Clearing Corporation (2018). *Systemic Risk Barometer: 2019 Forecast*. Systemic Risk Report, Depository Trust & Clearing Corporation (DTCC), New York.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 04(02), 92–100.

Financial Stability Board (2017). *Financial stability implication from FinTech: Supervisory and Regulatory Issues that Merit's Authorities' Attention*. Basel: Financial Stability Board (FSB). Source: http://www.fsb.org/wp-content/uploads/R270617.pdf.

Freund, J. & Jones, J. (2015). *Measuring and Managing Information Risk: A FAIR Approach*. Oxford: Elsevier.

Fritzvold, E. (2017). *Cyber Security in Organizations*. Master's thesis, University of Stavanger.

Han, J., Kamber, M., & Pei, J. (2012). *Data Mining Concept & Technique*. Waltham: Elsevier, 3rd edition.

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, 43, 248–260.

IIROC (2016). *Cybersecurity Best Practices Guide*. Cybersecurity guide, Investment Industry Regulatory Organization of Canada (IIROC), Toronto.

Iman, N. (2018). Assessing the dynamics of fintech in Indonesia. *Investment Management and Financial Innovations*, 15(4), 296–303.

ISO/IEC (2005). *Information technology - Security techniques - Information security management systems - Requirements*. ISO/IEC 27001:2005, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).

ISO/IEC (2012). *Information technology Security techniques Information security management systems Overview and Vocabulary*. ISO/IEC 27000:2012, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).

ISO/IEC (2013). *Information technology - Security techniques - Information security management systems - Requirements*. ISO/IEC 27001:2013, International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).

Kesswani, N. & Kumar, S. (2015). Maintaining Cyber Security: Implication, Cost and Returns. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 161–164).

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22, 113–122.

Landoll, D. J. (2011). *The Security Risk Assessment Handbook - A Complete Guide for Performing Security Risk Assessments*. Boca Raton: CRC Press, 2nd edition.

Lukonga, I. (2018). *Fintech , Inclusive Growth and Cyber Risks : A Focus on the MENAP and CCA Regions*. Working Paper WP/18/201, International Monetary Fund (IMF), Washington DC.

Marinos, L., Belmonte, A., & Rekleitis, E. (2016). *ENISA Threat Landscape 2015*. Research Report, European Union Agency For Network And Information Security. Source: https://www.enisa.europa.eu/publications/etl2015.

Nagaraju, V., Fiondella, L., & Wandji, T. (2017). A survey of fault and attack tree modeling and analysis for cyber risk management. *2017 IEEE International Symposium on Technologies for Homeland Security*.

OECD (2002). *OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*. Paris: Organisation for Economic Co-operation and Development (OECD).

Ostrom, L. T. & Wilhelmsen, C. A. (2012). *Risk Assessment: Tools, Techniques, and their Applications*. New Jersey: John Wiley & Sons.

Patil, P., Zavarsky, P., Lindskog, D., & Ruhl, R. (2012). Fault tree analysis of accidental insider security events. *International Conference on Cyber Security*, (pp. 113–118).

Pollari, I. & Ruddenklau, A. (2019). *ThePulse of Fintech 2018: Biannual global analysis of investment in fintech*. Biannual Report, Klynveld Peat Marwick Goerdeler (KPMG), Amstelveen.

PricewaterhouseCoopers (2017). *Redrawing the lines: Fintech's growing influence on Financial Services*. Global FinTech Report, PricewaterhouseCoopers (PWC).

Purwanegara, M., Apriningsih, A., & Andika, F. (2014). Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes. *Procedia - Social and Behavioral Sciences*, 115, 147–155.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management*. Cham: Springer.

Romãnova, I. & Kudinska, M. (2017). Banking and fintech: A challenge or opportunity? *Contemporary Studies in Economic and Financial Analysis*, 98, 21–35.

Schueffel, P. (2016). Taming the Beast: A Scientific Definition of Fintech. *SSRN*, (pp. 1–24).

Shojaie, B. (2018). *Implementation of Information Security Management Systems based on the ISO / IEC 27001 Standard in different cultures*. PhD thesis, Universität Hamburg.

Stallings, W. (2011). *Network Security Essentials: Application and Standards*. New Jersey: Prentice - Hall, 4th edition.

Tanuwidjaja, E. & Quan, Y. M. (2018). *Indonesia: Assessing the Digital Economy's Potential*. Global Economics & Market Research, United Overseas Bank (UOB).

Source: https://www.uobgroup.com/web-resources/uobgroup/pdf/research/MN_180718A.pdf.

Téllez, J. & Zeadally, S. (2017). *Mobile Payment Systems: Secure Network Architectures and Protocols*. Basel: Springer.

Wangen, G. B. (2017). *Cyber Security Risk Assessment Practices Core: Core Unified Risk Framework*. PhD thesis, Norwegian University of Science and Technology.

Wroblewska, A., Twardowski, B., Zawistowski, P., & Ryżko, D. (2016). Automatic Clustering Methods of Offers in an E-Commerce Marketplace. In D. Ryżko, P. Gawrysiak, M. Kryszkiewicz, & H. Rybiński (Eds.), *Machine Intelligence and Big Data in Industry* (pp. 147–160). Cham: Springer International Publishing.

Zavolokina, L., Dolata, M., & Schwabe, G. (2016). The FinTech phenomenon: antecedents of financial innovation perceived by the popular press. *Financial Innovation*, 2(1), 16.