Title

Enhancing cybersecurity capability investments: Evidence from an experiment

Abstract

In recent years, investments in cybersecurity capabilities (CC) have emerged as an essential practice in reducing cyberattacks and optimizing the usage of technologies. Therefore, optimal investments in capabilities must be determined according to the cybersecurity scenario of firms. This experiment pursues an understanding of the effectiveness of the iterative learning process in investments in CC. Through a simulator game, experienced and inexperienced participants overcome challenges related to uncertainties of cyber incidents to decision-making in cybersecurity capability investments. The collected data were empirically tested from 119 participants analyzing 3,808 simulation runs. The findings demonstrated that there is a slight difference in the learning curve between the two groups even if they learn proactively and iteratively. However, experienced, and inexperienced groups did not demonstrate enough capacity to analyze the cybersecurity ecosystems designed in the simulator game to mitigate cyber incidents. Both groups exhibited similar results regarding gaps to invest in CC to address uncertainties associated with cyber threats. In this sense, this experiment highlights the relevance of learning about CC investments in any context to avoid resource losses and time to uncover the complexities related to incident responses. © 2023 Elsevier Ltd

Authors

Pigola A.; Da Costa P.R.; Ferasso M.; Cavalcanti da Silva L.F.

Author full names

Pigola, Angélica (57236843700); Da Costa, Priscila Rezende (57396713900); Ferasso, Marcos (24279220200); Cavalcanti da Silva, Luís Fabio (58800108900)

Author(s) ID

57236843700; 57396713900; 24279220200; 58800108900

Year

2024

Source title

Technology in Society

Volume

76.0

Art. No.

102449

DOI

10.1016/j.techsoc.2023.102449

Link

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85181775436&doi=10.1016%2fj.techsoc.2023.102449&partnerID=40&md5=23919af5969c4e4e098e1d50369e5dad

Affiliations

Master and Doctoral Program in Administration, UNINOVE – University Nove de Julho, SP, São Paulo, 01525-000, Brazil; Escola de Ciências Económicas e das Organizações, Lusófona University, Campo Grande, 3761749-024, Lisboa, Portugal; Grupo de Investigación de Estudios Organizacionales Sostenibles, Universidad Autónoma de Chile, Santiago, Chile

Authors with affiliations

Pigola A., Master and Doctoral Program in Administration, UNINOVE – University Nove de Julho, SP, São Paulo, 01525-000, Brazil; Da Costa P.R., Master and Doctoral Program in Administration, UNINOVE – University Nove de Julho, SP, São Paulo, 01525-000, Brazil; Ferasso M., Escola de Ciências Económicas e das Organizações, Lusófona University, Campo Grande, 3761749-024, Lisboa, Portugal, Grupo de Investigación de Estudios Organizacionales Sostenibles, Universidad Autónoma de Chile, Santiago, Chile; Cavalcanti da Silva L.F., Master and Doctoral Program in Administration, UNINOVE – University Nove de Julho, SP, São Paulo, 01525-000, Brazil

Author Keywords

Cybersecurity; Dynamic capabilities; Experiment; Iterative learning; Simulation

Index Keywords

Cybersecurity; Decision making; Learning systems; Cyber security; Cyber-attacks; Decisions makings; Dynamics capability; Iterative learning; Iterative learning process; Learning curves; Optimal investments; Simulation; Uncertainty; computer simulation; experiment; information and communication technology; investment; learning; security; Investments

Funding Details

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, CAPES, (001)

Funding Texts

“This work was supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES), grant number 001 ”.

References

Fernandez De Arroyabe I., Arranz C.F.A., Arroyabe M.F., Fernandez De Arroyabe J.C., Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019, Comput. Secur., 124, (2023); D'Arcy J., Adjerid I., Angst C.M., Glavas A., Too good to be true: firm social performance and the risk of data breach, Inf. Syst. Res., 31, pp. 1200-1223, (2020);

Jalali M.S., Siegel M., Madnick S., Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment, J. Strat. Inf. Syst., 28, pp. 66-82, (2019); Kour R., Karim R., Cybersecurity workforce in railway: its maturity and awareness, J. Qual. Mainten. Eng., 27, pp. 453-464, (2020); Fleischman G.M., Valentine S.R., Curtis M.B., Mohapatra P.S., The influence of ethical beliefs and attitudes, norms, and prior outcomes on cybersecurity investment decisions, Bus. Soc., 62, pp. 488-529, (2023); Gupta R., Biswas B., Biswas I., Sana S.S., Firm investment decisions for information security under a fuzzy environment: a game-theoretic approach, ICS, 29, pp. 73-104, (2021); Cost of a Data Breach Report 2023, (2023); Shaikh F.A., Siponen M., Organizational learning from cybersecurity performance: effects on cybersecurity investment decisions, Inf. Syst. Front, (2023); Cavusoglu H., Mishra B., Raghunathan S., The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers, Int. J. Electron. Commer., 9, pp. 70-104, (2004); Chellappa R.K., Pavlou P.A., Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logistics Information Mngt., 15, pp. 358-368, (2002); Crossler R.E., Johnston A.C., Lowry P.B., Hu Q., Warkentin M., Baskerville R., Future directions for behavioral information security research, Comput. Secur., 32, pp. 90-101, (2013); Jalali M.S., Kaiser J.P., Cybersecurity in hospitals: a systematic, organizational perspective, J. Med. Internet Res., 20, (2018); Kalderemidis I., Farao A., Bountakas P., Panda S., Xenakis C., GTM: game Theoretic Methodology for optimal cybersecurity defending strategies and investments, Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1-9, (2022); Adams M., Makramalla M., Cybersecurity Skills Training: an Attacker-Centric Gamified Approach, Technology Innovation Management Review, (2015); Benz M., Chatterjee D., Calculated risk? A cybersecurity evaluation tool for SMEs, Bus. Horiz., 63, pp. 531-540, (2020); Kwon J., Johnson M.E., Proactive versus reactive security investments in the healthcare sector, MIS Q., 38, (2014); Kabanda S., Tanner M., Kent C., Exploring SME cybersecurity practices in developing countries, J. Organ. Comput. Electron. Commer., 28, pp. 269-282, (2018); Xu L., Li Y., Lin Y., Tang C., Yao Q., Supply chain cybersecurity investments with interdependent risks under different information exchange modes, Int. J. Prod. Res., pp. 1-26, (2023); Master A., Hamilton G., Dietz J.E., Optimizing cybersecurity budgets with AttackSimulation, 2022 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-7, (2022); Catota F.E., Granger Morgan M., Sicker D.C., Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, 5, pp. 1-19, (2019); Dhillon G., Smith K., Dissanayaka I., Information systems security research agenda: exploring the gap between research and practice, J. Strat. Inf. Syst., 30, (2021); Hwang M.I., Helser S., Cybersecurity educational games: a theoretical framework, ICS, 30, pp. 225-242, (2022); Khalid Khan S., Shiwakoti N., Stasinopoulos P., A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles, Accid. Anal. Prev., 165, (2022); Meland P.H., Bernsmed K., Froystad C., Li J., Sindre G., An experimental evaluation of bow-tie analysis for security, ICS, 27, pp. 536-561, (2019); Helfat C.E., Finkelstein S., Mitchell W., Peteraf M., Singh H., Teece D., Winter S.G., Dynamic Capabilities: Understanding Strategic Change in Organizations, (2009); Teece D.J., Pisano G., Shuen A., Dynamic capabilities and strategic management, Strat. Mgmt. J., 18, pp. 509-533, (1997); Zahra S.A., Sapienza H.J., Davidsson P., Entrepreneurship and dynamic capabilities: a review, model and research agenda, J. Manag. Stud., 43, pp. 917-955, (2006); Eisenhardt K.M., Martin J.A., Dynamic capabilities: what are they?, Strat. Mgmt. J., 21, pp. 1105-1121, (2000); Zollo M., Winter S.G., Deliberate learning and the evolution of dynamic capabilities, Organ. Sci., 13, pp. 339-351, (2002); Steininger D.M., Mikalef P., Pateli A., Ortiz-de-Guinea A., Dynamic capabilities in information systems research: a critical review, synthesis of current knowledge, and recommendations for future research, JAIS, 22, pp. 447-490, (2022); Piccoli I., Review: IT-dependent strategic initiatives and sustained competitive advantage: a review and synthesis of the literature, MIS Q., 29, (2005); Wade H., Review: the resource-based view and information systems research: review, extension, and suggestions for future research, MIS Q., 28, (2004); Amit R., Schoemaker P.J.H., Strategic assets and organizational rent: strategic Assets, Strat. Mgmt. J., 14, pp. 33-46, (1993); Barreto I., Dynamic capabilities: a review of past research and an agenda for the future, J. Manag., 36, pp. 256-280, (2010); Burisch R., Wohlgemuth V., Blind spots of dynamic capabilities: a systems theoretic perspective, J. Innovation & Knowledge, 1, pp. 109-116, (2016); Laaksonen O., Peltoniemi M., The essence of dynamic capabilities and their measurement: essence of dynamic capabilities, Int. J. Manag. Rev., 20, pp. 184-205, (2018); Al-Matouq H., Mahmood S., Alshayeb M., Niazi M., A maturity model for secure software design: a multivocal study, IEEE Access, 8, pp. 215758-215776, (2020); Introducing CMMI Security v2.0, (2019); Humayun M., Jhanjhi N., Fahhad Almufareh M., Ibrahim Khalil M., Security threat and vulnerability assessment and measurement in secure software development, Comput. Mater. Continua (CMC), 71, pp. 5039-5059, (2022); Ghobakhloo M., Fathi M., Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing, JMTM, 31, pp. 1-30, (2019); Eastman R., Versace M., Webber A., Big data and predictive analytics: on the cybersecurity front line, IDC Whitepaper, (2015); Naseer A., Naseer H., Ahmad A., Maynard S.B., Masood Siddiqui A., Real-time analytics, incident response process agility and enterprise cybersecurity performance: a contingent resource-based analysis, Int. J. Inf. Manag., 59, (2021); Naseer H., Maynard S.B., Desouza K.C., Demystifying analytical information processing capability: the case of cybersecurity incident response, Decis. Support Syst., 143, (2021); Kapoor A., Gupta A., Gupta R., Tanwar S., Sharma G., Davidson I.E., Ransomware detection, avoidance, and mitigation scheme: a review and future directions, Sustainability, 14, (2021); Tanwar S., Vora J., Tyagi S., Kumar N., Obaidat M.S., A systematic review on security issues in vehicular ad hoc network, Security and Privacy, 1, (2018);

Abdul Molok N.N., Ahmad A., Chang S., A case analysis of securing organisations against information leakage through online social networking, Int. J. Inf. Manag., 43, pp. 351-356, (2018); Goode S., Lacey D., Exploiting organisational vulnerabilities as dark knowledge: conceptual development from organisational fraud cases, JKM, (2021); Teece D.J., Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance, Strat. Mgmt. J., 28, pp. 1319-1350, (2007); Akinsanya O.O., Papadaki M., Sun L., Towards a maturity model for health-care cloud security, ICS, 28, pp. 321-345, (2019); Fagade T., Maraslis K., Tryfonas T., Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach, Int. J. Comput. Intell. Syst., 13, (2017); Madnick S., Jalali M.S., Siegel M., Lee Y., Strong D., Wang R., Ang W.H., Deng V., Mistree D., Measuring stakeholders' perceptions of cybersecurity for renewable energy systems, Data Analytics for Renewable Energy Integration, pp. 67-77, (2017); Chatterjee S., Thekdi S., An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems, Reliab. Eng. Syst. Saf., 193, (2020); Steinmetz K.F., Craft(y)ness: an ethnographic study of hacking, CRIMIN, 55, pp. 125-145, (2015); Xu F., Robert X., Luo, Zhang H., Liu S., Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect, Inf. Syst. Front, 21, pp. 1069-1083, (2019); Disparte D., Furlow C., The best cybersecurity investment you can make is better training, Harv. Bus. Rev., 5, (2017); Catal C., Ozcan A., Donmez E., Kasif A., Analysis of cyber security knowledge gaps based on cyber security body of knowledge, Educ. Inf. Technol., 28, pp. 1809-1831, (2023); McClain J., Silva A., Emmanuel G., Anderson B., Nauer K., Abbott R., Forsythe C., Human performance factors in cyber security forensic analysis, Procedia Manuf., 3, pp. 5301-5307, (2015); Cain A.A., Edwards M.E., Still J.D., An exploratory study of cyber hygiene behaviors and knowledge, J. Inf. Secur. Appl., 42, pp. 36-45, (2018); Zwilling M., Klien G., Lesjak D., Wiechetek L., Cetin F., Basim H.N., Cyber security awareness, knowledge and behavior: a comparative study, J.

Comput. Inf. Syst., 62, pp. 82-97, (2022); Daniel C., Mullarkey M., Agrawal M., RQ labs: a cybersecurity workforce skills development framework, Inf. Syst. Front, (2022); Beuran R., Vykopal J., Belajova D., Celeda P., Tan Y., Shinoda Y., Capability assessment methodology and comparative analysis of cybersecurity training platforms, Comput. Secur., 128, (2023); Zacharis A., Patsakis C., AiCEF: an AI-assisted cyber exercise content generation framework using named entity recognition, Int. J. Inf. Secur., 22, pp. 1333-1354, (2023); Van Der Kleij R., Schraagen J.M., Cadet B., Young H., Developing decision support for cybersecurity threat and incident managers, Comput. Secur., 113, (2022); Jalali M.S., How individuals weigh their previous estimates to make a new estimate in the presence or absence of social influence, Social Computing, Behavioral-Cultural Modeling and Prediction, pp. 67-74, (2014); Fisher C.W., Chengalur-Smith I., Ballou D.P., The impact of experience and time on the use of data quality information in decision making, Inf. Syst. Res., 14, pp. 170-188, (2003); Sterman J.D., System dynamics modeling: tools for learning in a complex world, Calif. Manag. Rev., 43, pp. 8-25, (2001); Jalali M.S., Ashouri A., Herrera-Restrepo O., Zhang H., Information diffusion through social networks: the case of an online petition, Expert Syst. Appl., 44, pp. 187-197, (2016); OliveiraJr E., Zorzo A.F., Neu C.V., Towards a conceptual model for promoting digital forensics experiments, Forensic Sci. Int.: Digit. Invest., 35, (2020); Mingers J., Standing C., A framework for validating information systems research based on a pluralist account of truth and correctness, JAIS, pp. 117-151, (2020); Morellato L.P.C., Alberti L.F., Hudson I.L., Applications of circular statistics in plant phenology: a case studies approach, Phenological Research, pp. 339-359, (2010); Sterman J.D., Franck T., Fiddaman T., Jones A., McCauley S., Rice P., Sawin E., Siegel L., Rooney-Varga J.N., World climate: a role-play simulation of climate negotiations, Simulat. Gaming, 46, pp. 348-382, (2015); Yang M.M., Jiang H., Gary M.S., Challenging learning goals improve performance in dynamically complex microworld simulations, Syst. Dynam. Rev., 32, pp. 204-232, (2016); McFarland L., Milstein B., Hirsch G., Homer J., Andersen D., Irving R., Reineke E., Niles R.D., Cawvey E., Desai A., MacDonald R., NASPAA student simulation competition: reforming the U.S. Health care system within a simulated environment, J. Publ. Aff. Educ., 22, pp. 363-380, (2016); Robinson S., Conceptual modelling for simulation Part I: definition and requirements, J. Oper. Res. Soc., 59, pp. 278-290, (2008); Pigola A., Enhancing Capabilities Development in Cybersecurity: Evidence from an Experiment, (2023); Rahmandad H., Impact of growth opportunities and competition on firm-level capability development trade-offs, Organ. Sci., 23, pp. 138-154, (2012); Rahmandad H., Weiss D.M., Dynamics of concurrent software development: H. Rahmandada and D. M. Weiss: dynamics of concurrent software development, Syst. Dynam. Rev., 25, pp. 224-249, (2009); Wang J., Gupta M., Rao H.R., Insider threats in a financial institution, MIS Q., 39, pp. 91-112, (2015); Willison R., Warkentin M., Beyond deterrence: an expanded view of employee computer abuse, MIS Q., pp. 1-20, (2013); Sangari S., Dallal E., Whitman M., Modeling reporting delays in cyber incidents: an industry-level comparison, Int. J. Inf. Secur., 22, pp. 63-76, (2023); Dinkova M., El-Dardiry R., Overvest B., Should firms invest more in cybersecurity?, Small Bus. Econ., (2023); Acquisti A., Grossklags J., Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior, 2nd Annual Workshop on Economics and Information Security-WEIS, pp. 1-27, (2003); Bowen B.M., Devarajan R., Stolfo S., Measuring the human factor of cyber security, 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 230-235, (2011); Sull D.N., Eisenhardt K.M., Simple Rules: How to Thrive in a Complex World, (2015); Bitzer M., Hackel B., Leuthe D., Ott J., Stahl B., Strobel J., Managing the inevitable – a maturity model to establish incident response management capabilities, Comput. Secur., 125, (2023); Karagiannis S., Magkos E., Adapting CTF challenges into virtual cybersecurity learning environments, ICS, 29, pp. 105-132, (2021); Shreeve B., Gralha C., Rashid A., Araujo J., Goulao M., Making sense of the unknown: how managers make cyber security decisions, ACM Trans.

Software Eng. Methodol., 32, pp. 1-33, (2023); Ekelund S., Iskoujina Z., Cybersecurity economics – balancing operational security spending, ITP, 32, pp. 1318-1342, (2019); Sewak M., Sahay S.K., Rathore H., Deep reinforcement learning in the advanced cybersecurity threat detection and protection, Inf. Syst. Front, (2022); Aleroud A., Abu-Shanab E., Al-Aiad A., Alshboul Y., An examination of susceptibility to spear phishing cyber-attacks in non-English speaking communities, J. Inf. Secur. Appl., 55, (2020); Workman M., Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, J. Am. Soc. Inf. Sci., 59, pp. 662-674, (2008); Zhang L., Zhu J., Liu Q., A meta-analysis of mobile commerce adoption and the moderating effect of culture, Comput. Hum. Behav., 28, pp. 1902-1911, (2012); Yamagishi T., Yamagishi M., Trust and commitment in the United States and Japan, Motiv. Emot., 18, pp. 129-166, (1994); Sharma K., Zhan X., Nah F.F.-H., Siau K., Cheng M.X., Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity, OCJ, 1, pp. 69-91, (2021); Barton K.A., Tejay G., Lane M., Terrell S., Information system security commitment: a study of external influences on senior management, Comput. Secur., 59, pp. 9-25, (2016); Bulgurcu C., Benbasat, information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q., 34, (2010); Hsu C., Lee J.-N., Straub D.W., Institutional influences on information systems security innovations, Inf. Syst. Res., 23, pp. 918-939, (2012); Pentland S.J., Twyman N.W., Burgoon J.K., Nunamaker J.F., Diller C.B.R., A video-based screening system for automated risk assessment using nuanced facial features, J. Manag. Inf. Syst., 34, pp. 970-993, (2017); Torres R., Sidorova A., Jones M.C., Enabling firm performance through business intelligence and analytics: a dynamic capabilities perspective, Inf. Manag., 55, pp. 822-839, (2018); Corte-Real N., Ruivo P., Oliveira T., Leveraging internet of things and big data analytics initiatives in European and American firms: is data quality a way to extract business value?, Inf. Manag., 57, (2020); Dukerich

J.M., Nichols M.L., Causal information search in managerial decision making, Organ. Behav. Hum. Decis. Process., 50, pp. 106-122, (1991); Paese P.W., Sniezek J.A., Influences on the appropriateness of confidence in judgment: practice, effort, information, and decision-making, Organ. Behav. Hum. Decis. Process., 48, pp. 100-130, (1991); Smith K.G., Grimm C.M., Gannon M.J., Chen M.-J., Organizational information processing, competitive responses, and performance in the U.S. Domestic airline industry, Acad. Manag. J., 34, pp. 60-85, (1991); Evans J.S.B.T., Hypothetical Thinking: Dual Processes in Reasoning and Judgement, (2007); Yang A., Kwon Y.J., Lee S.-Y.T., The impact of information sharing legislation on cybersecurity industry, IMDS, 120, pp. 1777-1794, (2020); Dong T., Zhu S., Oliveira M., Robert X., Luo, Making better IS security investment decisions: discovering the cost of data breach announcements during the COVID-19 pandemic, IMDS, 123, pp. 630-652, (2023); Demek K.C., Kaplan S.E., Cybersecurity breaches and investors' interest in the firm as an investment, Int. J. Account. Inf. Syst., 49, (2023); Wessels M., Van Den Brink P., Verburgh T., Cadet B., Van Ruijven T., Understanding incentives for cybersecurity investments: development and application of a typology, Digital Business, 1, (2021)

Correspondence Address

A. Pigola; Master and Doctoral Program in Administration, UNINOVE – University Nove de Julho, São Paulo, SP, 01525-000, Brazil; email: a_pigola@uni9.edu.br

Publisher

Elsevier Ltd

ISSN

0160791X

Language of Original Document

English

Abbreviated Source Title

Technol. Soc.

Document Type

Article

Publication Stage

Final

Source

Scopus

EID

2-s2.0-85181775436