Exploring Behavioural Strategies in Cyberinsurance Adoption

Yolanda Gómez
DevStat, Valencia, Spain

Dawn Branley-Bell*
Department of Psychology, Northumbria University, Newcastle upon Tyne, UK
dawn.branley-bell@northumbria.ac.uk

Pam Briggs
Department of Psychology, Northumbria University, Newcastle upon Tyne, UK

José Vila
Centre for Research in Social and Economic Behavior (ERI-CES), Laboratory for Intelligent Data Analysis (IDAL),Valencia, Spain

ABSTRACT

This study explores decision making around the purchase of cyberinsurance and the impact on cybersecurity behaviours. In an online experiment, involving 4,800 participants across four countries, we found that rational choice models fail to predict cybersecurity decisions. Specifically, individuals tend to opt for an overprotective cybersecurity strategy by ensuring higher protection levels and insurance coverage than expected utility theory would deem necessary. Two key implications are highlighted: Firstly, the need to focus on the human component of cybersecurity, and secondly, the need to develop behaviour-oriented interventions driven by theory and capable of accounting for the non-rational component of cybersecurity decision-making.

CCS CONCEPTS

• **Human-centered computing** → Human computer interaction (HCI); Empirical studies in HCI; • **Security and privacy** → Human and societal aspects of security and privacy.

KEYWORDS

cybersecurity, cyberinsurance, moral hazard, behavioral experiment

ACM Reference Format:
Yolanda Gómez, Dawn Branley-Bell, Pam Briggs, and José Vila. 2024. Exploring Behavioural Strategies in Cyberinsurance Adoption. In *European Conference on Cognitive Ergonomics (ECCE 2024), October 08–11, 2024, Paris, France.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3673805.3673816

1 INTRODUCTION

Cybersecurity is a global problem [1] and organisations can mitigate the threat of a cyberattack by three key interventions: improving their technical cybersecurity defenses, promoting better cybersecurity behaviours amongst staff [2] and adopting appropriate cyberinsurance. The first intervention (technical defense) is probably the most widely implemented, but the second (behaviour change) is also a critical strategy to improve cyber preparedness [3] given that attackers are increasingly aware that employees can provide the most effective entry point into company systems, even if sophisticated security technologies are in place [4]. The third intervention (cyberinsurance) could, in principle, strengthen IT security for society as a whole [5], [6]. However, studies have shown that only a small percentage of companies are adopting cyberinsurance [7] [8] and also that the decisions for adopting cyberinsurance are not always rational [9].

Irrational decisions may be driven by several factors, including a lack of insurance and/or cybersecurity literacy or the presence of systematic cognitive biases that affect judgements of vulnerability or that inflate self-efficacy beliefs. The cyberinsurance market operates in a state of information asymmetry: although some elements of the cybersecurity position of the company can be observed by insurers risk audits, many behavioural vulnerabilities can remain hidden. This information asymmetry can result in the insurer being unable to identify high-risk clients [10] and adverse selection may occur when this is exploited by potential clients, e.g., if those with the riskiest behaviour are more likely to purchase insurance. Thirdly, information asymmetry may make indetectable potential changes in the behaviour of the client after they have purchased their insurance policy. Insurance coverage could present an incentive for the insured client to behave in a more risky manner or reduce their other security measures (referred to as moral hazard) [10], [11]. As insurers will not run at a loss, this leads to a stalemate situation whereby insurance companies increase their policy prices in an attempt to mitigate risk, which then deters potential clients with safer behaviour from purchasing policies. Moral hazard has been demonstrated in relation to other types of insurance [12], [13]. However, some studies have disputed these claims and suggested that moral hazard may not apply in some circumstances [14], [15] furthermore it is also possible that advantageous selection could occur. Advantageous selection is possible if individuals who opt to purchase cyberinsurance tend to be more risk averse and seek to reduce risk across all domains of their decision-making and behaviour [16]. Therefore, results are conflicted whether the purchase of cyberinsurance may influence adoption of other protection measures and/or online behaviour in a positive or negative way. Utilising a large-scale online behavioural economic experiment, we

*Corresponding Author.

ECCE 2024, October 08–11, 2024, Paris, France

ACM ISBN 979-8-4007-1824-3/24/10
https://doi.org/10.1145/3673805.3673816

explore whether concerns around irrational cyberinsurance decisions, information asymmetry and/or moral hazard appear to be justified.

1.1 Rationale

As noted above, companies are able to use a combination of cyberinsurance, cyberprotection and behaviour change as part of their cybersecurity strategy and these dimensions are highly interdependent [17]. Cyberprotection and cyberinsurance factors should be studied together, as their purchase requires the allocation of a limited budget which is likely to be split amongst the two. Other decisions that relate to organisational posture (e.g., cybersecurity policies, cybersecurity culture) and employee behaviour (e.g., security compliance) are usually made after cyberprotection and cyberinsurance have been purchased, and so don't have direct budgetary implications, however human behaviour may be affected by previous purchase decisions. Companies make purchase decisions that can be modelled as standard consumer choice decision-making under uncertainty. From a rational choice perspective, company decisions will be determined by the available budget, the prices of the cybersecurity elements, perceived risk of suffering the attack and the utility function of the company [18]. A truly rational decision-maker would select the combination of cyberprotection and cybersecurity that maximises expected utility. However, naturalistic decision making is seldom rational [19] and decision-making is often influenced by cognitive biases and the use of heuristics (also known as mental shortcuts or 'rule of thumb' processes) that can lead to less-than-optimal choices [20]. For example, low probability events are vastly overweighed or ignored when deciding whether to purchase insurance [21]. Individuals may interpret insurance as a certain expense (i.e., cost of coverage and associated security measures, effort setting up the policy) for a non-certain benefit (i.e., coverage in the event of an attack; [22]). Lack of knowledge about benefits and coverage also results in consumers making poor insurance decisions [23]. Behavioural economics has questioned the capacity of the rational choice approach to explain actual cybersecurity decision-making [24]. This discussion motivates our first research hypothesis:

> H_1: The purchasing decision of cyberinsurance and cyberprotection products is not rational, i.e., the selection of the cybersecurity strategy is not driven by maximisation of the expected utility of the participants.

Insurers may require a minimum level of protection. Mandatory regulations that stipulate certain self-protection measures (similar to mandatory seat belts in cars) are a general requirement in the case of many critical infrastructure operators [10]. The idea of a minimum level of observable protection is also suggested by the UK National Cyber Security Centre (NCSC) within its Cyber Essentials scheme. Introduced in 2014, this government backed cybersecurity certification scheme sets out a recommended baseline of cybersecurity suitable for all organisations. The scheme addresses five key controls that, correctly implemented, can prevent around 80% of cyberattacks (firewall use, secure settings on devices and software, control over data access, antivirus protection and regular updating). However, beyond the basic Cyber Essentials or other insurer requirements, the insured can also choose to invest in additional non-compulsory protection measures. A common practice in the cyberinsurance industry, is the application of different pricing for the same insurance product depending on the organisation's self-protection level [10]. H_2 tests whether the application of these pricing strategies helps companies to make better decisions, from the viewpoint of rational choice theory [25]:

> H_2: If cyberprotection level can be observed by the insurer, variable pricing policies incentivising cyberprotection (i.e., with a cybersinsurance price reduction) enhances the rationality of the purchasing decision of cybersecurity products.

Businesses, particularly small and medium-sized enterprises (SMEs), can often be heavily restricted by the budget they have available for cybersecurity; because of this they are forced to make trade-offs regarding how they defend their systems [26]. When making this trade-off, the organisation must make a decision based upon the direct cost of implementing a particular safeguard and the impact that the safeguard may have on the business (e.g., indirect costs such as a reduction in productivity speed, morale cost or retraining cost [26]). At a certain level of protection, implementing additional controls/safeguards may only reduce vulnerability by a fraction of its maximum efficiency. Conversely, the cost of implementation remains the same, therefore there becomes a diminishing return for each control that you add to the system. In this context, our H_3 determines the relationship between cyberinsurance and additional protection:

> H_3: Cyberprotection and cyberinsurance products are complementary goods.

1.2 Online Behaviour

No matter the security products adopted by an organisation, employee error will always be a source of vulnerability, and humans are increasingly becoming the target of cyberattacks [27] [28] [29]. As previously discussed, it is imperative to analyse the relationship between online behaviour and cybersecurity within the frame of information asymmetry and/or moral hazard. The seminal work of Rothschild and Stiglitz [30] shows that individuals with private information (i.e., not known to the insurer) and higher risk are more prone to select insurance policies with a higher coverage level than those also with private information but a lower risk – suggesting adverse selection. However, other evidence conflicts with this viewpoint. For instance, research showing that 4.8% of UK credit cards were reported lost or stolen each year, whereas for insured cards the corresponding figure reduced to 2.7% [31] – suggestive of advantageous selection where insured individuals are acting more securely. In other words, individuals who adopt insurance may generally be more risk averse, whereas those who are reluctant to purchase insurance may be less risk adverse and therefore more likely to behave in a risky manner and less inclined to take precautionary security measures [31]. Furthermore, where moral hazard may be an issue, Gordon and Loeb [25] suggest that this can potentially be addressed by offering premium reductions for increases in security posture, and by imposing deductibles that ensure that the insured suffers some loss in the event of an incident (although due to the general unobservability of the insured's

behaviour, these measures cannot be easily implemented). Building from this empirical evidence in other insurance domains with asymmetric information and where the occurrence of the insured events has a critical impact (e.g., health, fraud), our next research hypotheses state that individuals who acquire cyberinsurance (H4) and/or implement advanced cyberprotection (H5) will also act more securely online. Specifically:

> H_4: Individuals who have acquired cyberinsurance with a higher coverage will behave more securely online.
>
> H_5: Individuals who have acquired safer cyberprotection products will behave more securely online.

2 METHOD AND EXPERIMENTAL DESIGN

An online behavioural study was designed to measure cyberinsurance and cyberprotection purchase decisions and related behaviours. Participants were asked to make cyberinsurance and cyberprotection purchase decisions before undertaking an online transaction where a number of behavioural security measures were recorded.

2.1 Procedure

Participants were initially given an endowment and informed that final payoff would be dependent upon their cybersecurity performance on the task. After receiving this information, they were offered the opportunity to spend part of their endownment to purchase different types of cyberprotection measures and cyberinsurance policies (with different prices and coverages in case of attack). In relation to cyberprotection measures, participants could choose between Basic Security Measures (BSMs – no cost, no change to probability of attack) and Advance Security Measures (ASMs – required investing their endowment, but resulted in the probability of an attack being reduced by half). Participants could opt to buy a cyberinsurance policy, either basic (cheaper but lower payout) or premium (more expensive but provides higher coverage). An example of the online shop screen is shown in Figure 1.

After purchasing their chosen cyberprotection and insurance options, participants were asked to complete an online task. The task was to register for a conference and whilst completing their registration, four security behaviours were measured: 1. Security of chosen password, 2. Whether the participant disclosed non-compulsory private information, 3. Whether they viewed the terms and conditions, and 4. Whether they clicked 'log out' after registering. Participants knew that their probability of suffering a cyberattack would be affected by how securely they behaved during the task, although they were not given details. The final payoff of each participant was computed as the sum of the remaining endowment (i.e., the initial endowment minus the cost of cyberprotection and cyberinsurance products purchased by the participant) and the assumed commercial profit (if no cyberattack) or insurance payout (if the cyberattack occurs).

2.2 Treatments

There were two experimental manipulations in the original study: (i) the *pricing strategy* applied to the cyberprotection and cyberinsurance products and (ii) the *Intentionality of the attack (random or targeted)*. In this paper, we present only the results relevant to the first factor (pricing strategy), which had six levels obtained from a combination of the following two factors: Cyberinsurance price level and price dependency. Cyberinsurance price had three levels: medium, asymmetric, and high. Price dependency had two levels: dependent price (insurance price reflected chosen security measures) and independent price (chosen security measures had no effect on insurance price).

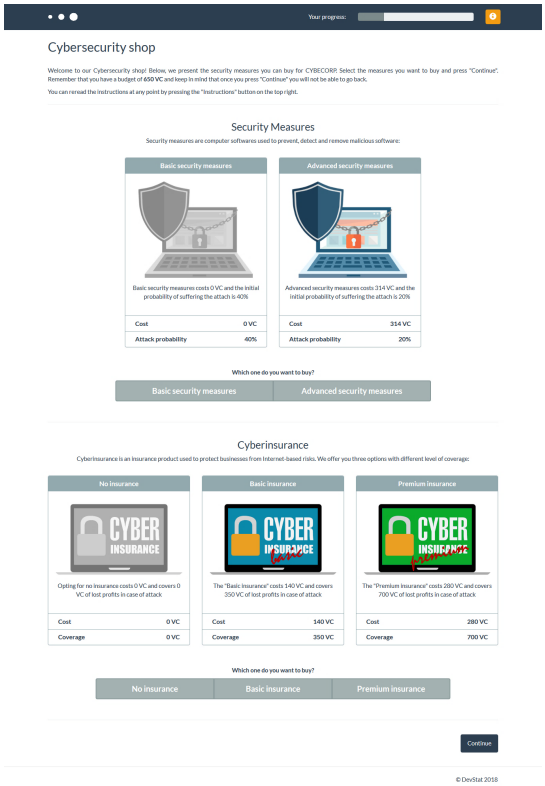

Figure 1: Example of Experimental Online Shop

2.3 Behavioural measures

Three behavioural measures were obtained: (i) security measures adoption (basic or advanced), (ii) insurance adoption (none, basic or premium) and online behaviour during the conference registration task. Online behaviour is calculated as a continuous variable between 0 (safest behaviour) and 1 (riskiest behaviour) as a linear combination of the proxy security variables included in the experiment: security level of chosen password, disclosure of non-compulsory private information, viewing the terms and conditions and logging out.

2.4 Participant Sample

A total of 4800 participants were recruited through the Online Panel of BDI Barcelona, to a quota balanced by country gender and age. Participants were regular internet users who had used the internet to purchase online products or services in the last year (to ensure familiarity with online purchases). Any participants completing the

Table 1: Participant Demographics

	Germany		*Spain*		*Poland*		*UK*	
	N	%	n	%	N	%	n	%
Male	617	51.42	600	50.00	552	46.00	595	49.58
Female	583	48.58	600	50.00	648	54.00	605	50.42
16 – 34yr	932	77.67	842	70.17	713	59.42	844	70.33
35 – 74yr	268	22.33	358	29.83	487	40.58	356	29.67
Total	*1200*	*100.00*	*1200*	*100.00*	*1200*	*100.00*	*1200*	*100.00*

Education level	n	%	Work Status	n	%
Compulsory	403	8.40	Worker	2808	58.50
Further	1446	30.12	Self-employed	452	9.42
Higher	2951	61.48	Other	1540	32.08
Total	4800	100.00	Total	4800	100.00

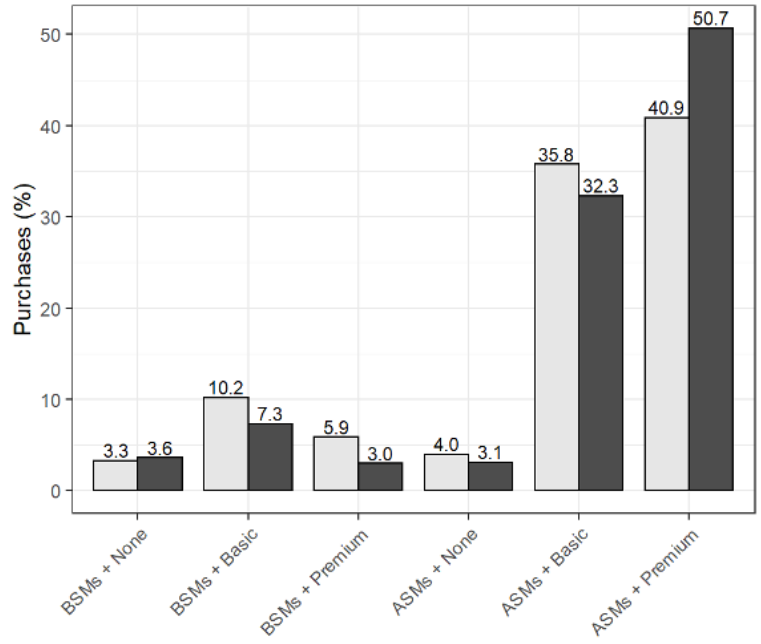

Figure 2: Cybersecurity strategy (Independent price group shown in light grey, dependent price group in dark grey)

experiment in less than 1/3 of the median time taken were removed from the sample and the quota was then re-opened. Table 1 shows the demographic distribution.

3 RESULTS

3.1 Cybersecurity strategy

The cybersecurity strategy (combination of cyberinsurance and cyberprotection measures) chosen by participants is represented in Figure 2. The results show both price dependency groups (dependent and independent). In both groups, the highest cybersecurity strategy, i.e., advanced security measures and premium insurance, was the most chosen strategy.

When the price was independent, the purchase of ASMs was never the best choice from a rational choice perspective. Considering this, the best combination was purchased by only 5.3% of participants in the independent price group. This percentage significantly increased to 8% in the dependent price group ($p<.05$). These results support our first hypothesis: Participants do not make optimal purchases of cyberinsurance and cyberprotection from a rational choice perspective (H_1). IOf those participants who purchased premium insurance, the majority (91.2%) also purchased

ASMs. This dropped to 79.5% for those who purchased basic insurance, and 50.9% for those who did not purchase any insurance ($p<.001$). The combination of the products therefore appears to be complementary: insurance does not substitute protection (supporting H_2). Finally, the application of price dependency helps participants to make more rational decisions (supporting H_3).

3.2 Impact of cybersecurity strategy on online behaviour

Two ANOVA models were estimated to test the effects of chosen security measures and cyberinsurance on online behaviour. Participants who purchased advanced SMs behaved more securely during the online task ($p<.001$). No significant effect was found for the purchase of cyberinsurance on online behaviour ($p = 0.20$). H_4 is supported – individuals who adoption advanced security measures behave more securely online. However, H_5 is not supported, the purchase of cyberinsurance did not affect behaviour.

4 DISCUSSION

Our results show that the Rational Choice Model fails to explain cybersecurity decisions. Individuals will opt for an overprotective cybersecurity strategy by selecting higher protection levels and insurance coverage than those that maximise their expected utility. Whilst our findings reinforce the existing literature that humans do not act according to the rational choice model [32], they also expand upon them by utising an economic experiment - within the cybersecurity context - to experimentally measure differences in behaviour, and demonstrate that concerns around individuals underinsuring and/or acting less securely after adoption (moral hazard) may be overstated.

These findings highlight the importance of a behavioural economics approach to analysing cyberinsurance adoption and encourages development of alternative behavioural models that do not assume perfect rationality. Our findings suggest that making protection levels of potential clients' observable to insurers (so that this can be reflected in policy premiums) is an effective strategy to help clients maximise their expected utility. As an extreme application, this finding supports public regulations and insurers pricing policies requiring a minimum level of protection.

We demonstrate that cyberprotection and cyberinsurance coverage are not substitutive but rather are complementary goods. In other words, the adoption of a higher level of insurance coverage is not associated with a lower level of cyberprotection. Strongly insured participants adopt more advanced cyberprotection measures – suggestive of advantageous selection. Furthermore, cyberinsurance adoption does not have an adverse effect on the security of the insured's subsequent online behaviour. Even when behaviour is not observable by the insurer, cyberinsurance coverage is not associated with any increase in insecure behaviour. Beyond scientific interest, these two findings have further implications for industry and policy, since a company's adoption of cyberinsurance or cyberprotection measures should not reduce the security of staff's behaviour, although we should note the caveat that our findings are derived from a laboratory, rather than a real-world study which may mean that our participants were primed to behave more securely than in a naturalistic setting.

In summary, our research provides empirical evidence suggesting that the growth of the cyberinsurance industry will not compromise the cyber-resilience of individuals and of the Digital Single Market. Deviations from maximum expected utility in our data translated into overprotection and overinsurance behaviours, which, whilst not optimal for insured individuals, actually increase the resilience of the digital system. Additionally, our findings suggest that information asymmetries in the cyberinsurance market would not result in insured individuals reducing their level of protection or adopting riskier online behaviour. We noted higher levels of protection and safer online behaviour among those who adopted cyberinsurance. Therefore, our results encourage further development of the cyberinsurance market and discredit moral hazard and adverse selection concerns.

ACKNOWLEDGMENTS

This work was supported by the European Union's Horizon 2020 research and innovation programme [grant no.740920].

REFERENCES

[1] [1]'The Global Risks Report', World Economic Forum, 2022. [Online]. Available: www.wef.ch/risks22
[2] [2]R. van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, 'Using protection motivation theory in the design of nudges to improve online security behavior', *International Journal of Human-Computer Studies*, vol. 123, pp. 29–39, Mar. 2019, doi: 10.1016/J.IJHCS.2018.11.003.
[3] [3]M. A. Sasse, S. Brostoff, and D. Weirich, 'Transforming the "weakest link" - A human/computer interaction approach to usable and effective security', *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001, doi: 10.1023/A:1011902718709.
[4] [4]B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, 15th Anniversary edition. Indianapolis, Indiana: Wiley, 2015.
[5] [5]W. S. Baer and A. Parkinson, 'Cyberinsurance in IT Security Management', *IEEE Security & Privacy Magazine*, vol. 5, no. 3, pp. 50–56, May 2007, doi: 10.1109/MSP.2007.57.
[6] [6]D. Kuru and S. Bayraktar, 'The effect of cyber-risk insurance to social welfare', *Journal of Financial Crime*, vol. 24, no. 2, pp. 329–346, May 2017, doi: 10.1108/JFC-05-2016-0035.
[7] [7]'Cyber Security Breaches Survey', GOV.UK. Accessed: May 15, 2023. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020
[8] [8]'The Hiscox Cyber Readiness Report', Hiscox UK. Accessed: May 15, 2023. [Online]. Available: https://www.hiscox.co.uk/cyberreadiness
[9] [9]D. R. Insua, C. Baylon, and J. Vila, *Security Risk Models for Cyber Insurance*. CRC Press, 2020.
[10] [10]D. Young, J. Lopez Jr., M. Rice, B. Ramsey, and R. McTasney, 'A framework for incorporating insurance in critical infrastructure cyber risk strategies', *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 43–57, Sep. 2016, doi: 10.1016/J.IJCIP.2016.04.001.
[11] [11]M. Eling and W. Schnell, 'What do we know about cyber risk and cyber risk insurance?', *The Journal of Risk Finance*, vol. 17, no. 5, pp. 474–491, Nov. 2016, doi: 10.1108/JRF-09-2016-0122.
[12] [12]J. Tolvanen, 'Measuring moral hazard using insurance panel data', 2015.
[13] [13]C. Sapelli and B. Vial, 'Self-selection and moral hazard in Chilean health insurance', *Journal of Health Economics*, vol. 22, no. 3, pp. 459–476, May 2003, doi: 10.1016/S0167-6296(02)00121-2.
[14] [14]P. Chiappori and B. Salanie, 'Testing for Asymmetric Information in Insurance Markets', *Journal of Political Economy*, vol. 108, no. 1, pp. 56–78, Feb. 2000, doi: 10.1086/262111.
[15] [15]T. Zavadil, 'Do the Better Insured Cause More Damage? Testing for Asymmetric Information in Car Insurance', *Journal of Risk and Insurance*, vol. 82, no. 4, pp. 865–889, Dec. 2015, doi: 10.1111/jori.12040.
[16] [16]P. Hudson, W. J. Wouter Botzen, J. Czajkowski, and H. Kreibich, 'Adverse Selection and Moral Hazard in Natural Disaster Insurance Markets: Empirical evidence from Germany and the United States', *Land Economics*, vol. 93, no. 2, pp. 179–208, 2017.
[17] [17]J. Bolot and M. Lelarge, 'Cyber Insurance as an Incentive for Internet Security', in *Managing Information Risk and the Economics of Security*, M. E. Johnson, Ed., Boston, MA: Springer US, 2009, pp. 269–290. doi: 10.1007/978-0-387-09762-6_13.
[18] [18]P. P. Wakker, *Prospect Theory*. Cambridge University Press, 2010. Accessed: May 15, 2023. [Online]. Available: https://www.cambridge.org/core/books/

prospect-theory/971C92E9EADA3FAECE7AE94126E4CEB1

[19] [19]G. A. Klein and R. Calderwood, 'Decision models: some lessons from the field', *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 21, no. 5, pp. 1018–1026, Sep. 1991, doi: 10.1109/21.120054.

[20] [20]T. Gilovich, D. Griffin, and D. Kahneman, Eds., *Heuristics and Biases: The Psychology of Intuitive Judgment*. Cambridge: Cambridge University Press, 2002. doi: 10.1017/CBO9780511808098.

[21] [21]A. Tversky and D. Kahneman, 'Advances in Prospect Theory: Cumulative Representation of Uncertainty', *Journal of Risk and Uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.

[22] [22]K. Baicker, W. J. Congdon, and S. Mullainathan, 'Health Insurance Coverage and Take-Up: Lessons from Behavioral Economics', *Milbank Quarterly*, vol. 90, no. 1, pp. 107–134, Mar. 2012, doi: 10.1111/j.1468-0009.2011.00656.x.

[23] [23]G. Loewenstein *et al.*, 'Consumers' misunderstanding of health insurance', *Journal of Health Economics*, vol. 32, no. 5, pp. 850–862, Sep. 2013, doi: 10.1016/j.jhealeco.2013.04.004.

[24] [24]F. Farahmand, 'Quantitative Issues in Cyberinsurance: Lessons From Behavioral Economics, Counterfactuals, and Causal Inference', *IEEE Security & Privacy*, vol. 18, no. 2, pp. 8–15, Mar. 2020, doi: 10.1109/MSEC.2019.2930054.

[25] [25]L. A. Gordon and M. P. Loeb, 'The economics of information security investment', *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002, doi: 10.1145/581271.581274.

[26] [26]A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, 'Decision support approaches for cyber security investment', *Decision Support Systems*, vol. 86, pp. 13–23, Jun. 2016, doi: 10.1016/J.DSS.2016.02.012.

[27] [27]K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, 'Human factor, a critical weak point in the information security of an organization's Internet of things', *Heliyon*, vol. 7, no. 3, p. e06522, Mar. 2021, doi: 10.1016/j.heliyon.2021.e06522.

[28] [28]M. Evans, Y. He, I. Yevseyeva, and H. Janicke, 'Analysis of Published Public Sector Information Security Incidents and Breaches to Establish the Proportions of Human Error', in *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 2018. [Online]. Available: https://books.google.co.uk/books?hl$=$en&lr$=$&id$=$XXRvDwAAQBAJ&oi$=$fnd&pg$=$PA191&dq$=$Evans,+He,+Yevseyeva,+and+Janicke+(2018)+&ots$=$_olzvyX2AH&sig$=$NGmyjVY3aOht6LgFc7MgQ-MAsr8#v$=$onepage&q$=$Evans%2C He%2C Yevseyeva%2C and Janicke (2018)&f=false

[29] [29]'ENISA Threat Landscape for Ransomware Attacks', ENISA, Report/Study, 2022. Accessed: May 15, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[30] [30]M. Rothschild and J. Stiglitz, 'Equilibrium in Competitive Insurance Markets: An essay on the economics of imperfect information', in *Uncertainty in Economics*, P. Diamond and M. Rothschild, Eds., Academic Press, 1978, pp. 257–280. doi: 10.1016/B978-0-12-214850-7.50024-3.

[31] [31]D. de Meza and D. C. Webb, 'Advantageous Selection in Insurance Markets', *The RAND Journal of Economics*, vol. 32, no. 2, pp. 249–262, 2001, doi: 10.2307/2696408.

[32] [32]J. Bone, 'Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I', *EDPACS*, vol. 54, no. 5, pp. 1–11, Nov. 2016, doi: 10.1080/07366981.2016.1247564.