11-2019

Choosing protection: User investments in security measures for cyber risk management

Yoav Ben YAAKOV

Xinrun WANG
Singapore Management University, xrwang@smu.edu.sg

Joachim MEYER

Bo AN

Citation

YAAKOV, Yoav Ben; WANG, Xinrun; MEYER, Joachim; and AN, Bo. Choosing protection: User investments in security measures for cyber risk management. (2019). *Decision and Game Theory for Security: 10th International Conference, GameSec 2019, Stockholm, October 30 – November 1: Proceedings*. 11836, 33-44.

Available at: https://ink.library.smu.edu.sg/sis_research/9150

Choosing Protection: User Investments in Security Measures for Cyber Risk Management

Yoav Ben Yaakov[1], Xinrun Wang[2], Joachim Meyer[1(✉)], and Bo An[2]

[1] Tel Aviv University, 69978 Tel Aviv, Israel
yoavbny@gmail.com, jmeyer@tau.ac.il
[2] Nanyang Technological University, Singapore, Singapore
{xwang033,boan}@ntu.edu.sg

Abstract. Firewalls, Intrusion Detection Systems (IDS), and cyber-insurance are widely used to protect against cyber-attacks and their consequences. The optimal investment in each of these security measures depends on the likelihood of threats and the severity of the damage they cause, on the user's ability to distinguish between malicious and non-malicious content, and on the properties of the different security measures and their costs. We present a model of the optimal investment in the security measures, given that the effectiveness of each measure depends partly on the performance of the others. We also conducted an online experiment in which participants classified events as malicious or non-malicious, based on the value of an observed variable. They could protect themselves by investing in a firewall, an IDS or insurance. Four experimental conditions differed in the optimal investment in the different measures. Participants tended to invest preferably in the IDS, irrespective of the benefits from this investment. They were able to identify the firewall and insurance conditions in which investments were beneficial, but they did not invest optimally in these measures. The results imply that users' intuitive decisions to invest resources in risk management measures are likely to be non-optimal. It is important to develop methods to help users in their decisions.

Keywords: Decision making · Cyber insurance · Cybersecurity

1 Introduction

1.1 Cybersecurity

Cybersecurity has become one of the major challenges for modern society [1], as the frequency and variety of cyber-attacks are steadily increasing [19], and the damage caused by cybercrime continues to rise [3]. The growing threats lead to a corresponding growth in the development of cybersecurity defense tools. The investment in these tools aims to diminish the risk of losses to the point where

T. Alpcan et al. (Eds.): GameSec 2019, LNCS 11836, pp. 33–44, 2019.
https://doi.org/10.1007/978-3-030-32430-8_3

the marginal cost of implementing security is equal to the additional reduction of the costs, caused by security incidents [8].

Organizations need to decide how to allocate resources to different risk mitigation measures. Such decisions are based on the evaluation of the efficiency of the different security measures by decision makers in organizations. Investment decisions regarding different security measures are complicated by the fact that the consequences of implementing one measure may affect the efficiency of others. Also, securing the cyberspace is not only a technical issue [12]. Rather, it is strongly affected by the behaviors, perceptions and decision making of the people who use these systems [7].

1.2 User Decision Making

To design proper security systems, designers must understand how users make decisions regarding security [20]. Actual human decisions regarding risk taking do not always correspond with the optimal decisions, prescribed by decision theory [20]. These deviations can result from users' evaluations of the trade-off between the effectiveness of the security and the usability of the system [15]. Some users may be willing to accept high False Alarm rates of an alerting system, if they think that the expected damage from an undetected malicious event is sufficiently larger than the expected cost of taking unnecessary actions after False Alarms. Others may prefer low False Alarm rates, if alerts are seen as too disruptive, even at the cost of reducing the likelihood of detecting an attack [2].

Also, decisions may not be optimal because abstract outcomes tend to have less impact on decisions than concrete ones [4]. In security, the pro-security alternative (invest in a security mechanism) usually has the invisible outcome of protecting from attacks [20]. This benefit is often intangible for users, making it difficult to evaluate the gains, compared to the costs. The difficulty to assess the benefits, gained from investing in security, is particularly large when users do not know the exact level of risk they are facing, or when they believe the risk is smaller than it actually is [20].

Risk taking is a complex combination of behaviors. It depends on the person's individual characteristics, on the available security mechanisms and information and on the nature of threats [2]. For instance, people who feel better protected are likely to engage in more risky behavior [20]. A person may take greater risks, knowing that a warning system is installed and no warning has been issued [13].

1.3 Defending Against Cyber-Threats

To lower risks, people can either reduce the likelihood of a threat or reduce the severity of the damage, caused by a successful attack. Firewalls are a widely used mechanism to lower the likelihood of threats. They are barriers between the secured and controlled internal networks and the untrusted outside networks [9]. The quality of a firewall system is measured by its ability to stop malicious events from entering the system, while not interfering with non-malicious events [8].

Cyber-insurance limits the damage caused by a cyber-attack, once it has occurred. It does not protect from attacks, but it helps organizations or individuals reduce their risks by sharing the costs associated with recovery after a successful cyber-attack [10].

One can also reduce risks by providing users with information that allows them to detect and avoid risks, using decision support systems or alerting systems. The availability of additional information may change the strategies decision makers use to address a decision problem [6]. In the context of cyber security, Intrusion Detection System (IDS) are widely used. They monitor networks or systems for malicious activity or policy violations, and they issue alerts when suspicious events are detected [8]. The quality of an IDS system is measured in terms of its ability to distinguish between malicious and non-malicious events. From the user's perspective, the IDS can improve the information the user has for deciding whether an event is malicious or not.

1.4 Our Contributions

We develop a model of the value of the investments, leading to the lowering of the likelihood of adverse events, the costs related to the adverse events, and the information available for detecting adverse events.

These three security measures affect different parts of the coping with threats, but they are intricately related. For instance, lowering the chances for the occurrence of adverse events may lower the need for investment in improved decision support. Thus, decision makers may need to consider trade-offs when deciding on the optimal strategy to manage cyber risks.

We also conducted a behavioral experiment to assess actual user behavior in a controlled lab setting and to compare it to the model predictions. The results of the study allow us to identify possible differences between user preferences and choices and the optimal security behavior, prescribed by the normative model. In particular, we aim to determine whether users respond more strongly and are more sensitive to the likelihood of damage or to its severity. We also observe whether users are able to choose the optimal investment in the alerting system, considering the properties of the system. The knowledge of such biased decisions can help us decide whether choices of risk-mitigation investments can be left to the user's intuitive choices, or whether one needs to develop ways to help users choose optimal protection.

2 Model

2.1 Modeling Framework

We use Signal Detection Theory (SDT) [11,16–18] to describe and study binary classification decisions under uncertainty. It assumes that classifications are made by deciding from which of two overlapping distributions (often referred to as signal and noise) an observation was sampled [21].

Signal detection theory commonly assumes Gaussian distributions. However, to facilitate the development of analytical solutions, we use Exponential distributions to represent the signal and noise.

2.2 Model Description

We consider a decision-making model of an agent (a company, an organization or an individual) in a given period (e.g., a year) to decide on cyber risk management. We consider three security measures for cyber risk management - firewalls, intrusion detection systems (IDS) and cyber-insurance. They become active sequentially - a threat first has to pass the firewall. It may then be detected by the IDS, and the user can respond to the indication of the IDS. The cyber-insurance will lower the damage, if neither of these two security measures stops the threat, and an attack occurs.

2.3 Firewall and IDS

Consider an information asset of the company with value v, which is also the loss caused when an attack succeeds. Let N be the number of events trying to access the information asset in the given period and ϵ of them are malicious, which can be estimated from the historical data. We assume the asset is protected by the typical cybersecurity system architecture. IDSs will raise an alarm when an event is identified as "malicious". The outputs of IDSs, together with the features of the events, are inputs to humans' classification decisions.

We use P_m^F to denote the probability that a malicious event can pass the firewall, which depends on the agent's investment in firewalls, yielding $P_m^F = f(x)$. We assume that all non-malicious events can pass the firewall. Therefore, the probability that an event that passed the firewall is malicious is

$$P_s = P(\text{Malicious}|\text{after Firewall}) = \frac{\epsilon \cdot P_m^F}{(1-\epsilon) + \epsilon \cdot P_m^F} \tag{1}$$

and the probability that the event is non-malicious is $P_n = 1 - P_s$. The probability that the IDS correctly detects a malicious event (i.e., true positive) is P_{TP}^I and P_{FP}^I is the probability that the IDS incorrectly classifies an event as malicious (i.e., false positive). The probabilities of false negative and true negative are denoted by $P_{FN}^I = 1 - P_{TP}^I$ and $P_{TN}^I = 1 - P_{FP}^I$, respectively. The values of $\langle P_{TP}^I, P_{FP}^I \rangle$ depend on the agent's investment in the IDS and the agent's alarming threshold β^I according to the signal detection theory (SDT) parameters $\langle \lambda_s, \lambda_n \rangle$, displayed in Fig. 1.

We can compute the probability that an event is malicious when the alarm is raised, i.e., the positive predicted value (PPV), and the probability that the event is non-malicious when the alarm is not raised, i.e., the negative predicted value (NPV).

$$PPV = P(\text{Malicious}|\text{Alarm}) = \frac{P^I_{TP}P_s}{P^I_{TP}P_s + P^I_{FP}P_n} \tag{2}$$

$$NPV = P(\text{Non-Malicious}|\text{No-Alarm}) = \frac{P^I_{TN}P_n}{P^I_{TN}P_n + P^I_{FN}P_s} \tag{3}$$

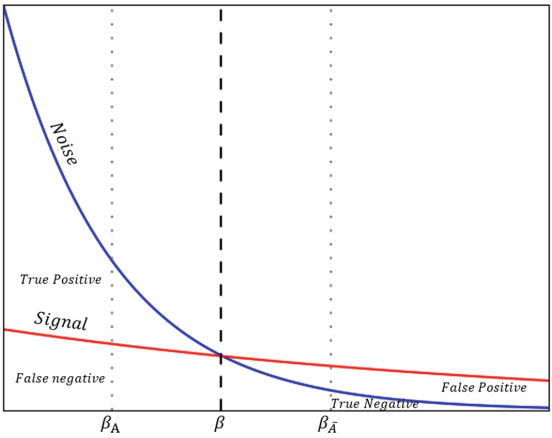

Fig. 1. Signal detection theory distributions for categorization decisions. The two exponential distributions for non-malicious and malicious events are parameterized by $\langle \lambda_s, \lambda_n \rangle$, respectively. W.l.o.g., we assume that $\lambda_s < \lambda_n$. The threshold β^I indicates that events with values above β^I will trigger an alarm in the IDS. When applying the model to the human monitoring decisions, β^H_A is the human threshold when an alarm was raised and $\beta^H_{\bar{A}}$ is the human threshold when no alarm was raised.

2.4 Human Monitoring

The human monitoring specifies the agent's monitoring policy, considering the company's defense systems (firewall and IDS). The agent classifies the event as malicious or non-malicious, given the output of the IDS, i.e., *alarm* and *no-alarm*. The payoff matrix of the agent consist of (i) if the event is malicious and the agent classifies it as "malicious", the agent suffers $-\gamma v$, (ii) if the event is non-malicious and the agent classifies it as "malicious", the agent suffers $-c$, (iii) if the event is malicious and the agent classifies it as "non-malicious", the agent suffers $-v$ and (iv) if the event is non-malicious and the agent classifies it as "non-malicious", the outcome is d. We note that $0 \leq \gamma < 1$ and $c < v$. The agent's monitoring policy is also modeled by SDT with the additional outputs, and the decision variables are $\langle \beta^H_A, \beta^H_{\bar{A}} \rangle$, which specifies the thresholds to classify the alarmed and no-alarmed events, as displayed in Fig. 1.

2.5 Cyber Insurance

The agent can purchase cyber insurance from an insurer with a premium to cover all (or a fraction of) the damage caused by the malicious events. The set

of insurances provided by the insurer is denoted by I and each insurance $I_i \in I$ is specified by P_i, L_i where P_i is the premium and L_i is the limit of liability. The insurer will not pay more than the limit of liability. The agent's strategy is denoted by z, where $z_i = 1$ if I_i is purchased and $z_i = 0$ otherwise.

2.6 Combining the Security Measures

After specifying the investments $\langle x, y, z\rangle$ and the thresholds $\langle \beta^I, \beta^H_A, \beta^H_{\bar{A}}\rangle$, we can compute the agent's expected costs, caused by an event that passes the firewalls.

$$
\begin{aligned}
&\hat{u}(x, y, z; \beta^I, \beta^H_A, \beta^H_{\bar{A}}) \\
&= P_A \cdot \{P(\text{Malicious}|\text{Alarm})[P^H_{TP|A}(-\gamma v) + P^H_{FN|A}(-v)]\} \\
&\quad + P_A \cdot \{P(\text{Non-Malicious}|\text{Alarm})[P^H_{FP|A}(-c) + P^H_{TN|A}(d)]\} \\
&\quad + P_{\bar{A}} \cdot \{P(\text{Malicious}|\text{No-Alarm})[P^H_{TP|\bar{A}}(-\gamma v) + P^H_{FN|\bar{A}}(-v)]\} \\
&\quad + P_{\bar{A}} \cdot \{P(\text{Non-Malicious}|\text{No-Alarm})[P^H_{FP|\bar{A}}(-c) + P^H_{TN|\bar{A}}(d)]\} \\
&= P^I_{TP} P_s [P^H_{TP|A}(-\gamma v) + P^H_{FN|A}(-v)] + P^I_{FP} P_n [P^H_{FP|A}(-c) + P^H_{TN|A}(d)] \\
&\quad + P^I_{FN} P_s [P^H_{TP|\bar{A}}(-\gamma v) + P^H_{FN|\bar{A}}(-v)] + P^I_{TN} P_n [P^H_{FP|\bar{A}}(-c) + P^H_{TN|\bar{A}}(d)] \quad (4)
\end{aligned}
$$

where P_A is the probability that an event will cause an alarm when passing the IDS. Therefore, the agent's damage, caused by all events, can be computed as $\hat{U}(x, y, z; \beta^I, \beta^H_A, \beta^H_{\bar{A}}) = N(\epsilon P^F_m + (1 - \epsilon)) \cdot \hat{u}(x, y, z; \beta^I, \beta^H_A, \beta^H_{\bar{A}})$. The agent's expected utility is

$$
U = \min\left\{0, \sum\nolimits_{I_i \in \mathcal{I}} z_i \cdot L_i - \bar{U}\right\} - I(B) \cdot \tilde{U} \quad (5)
$$

with the constraint that

$$
\tilde{U} \leq B \quad (6)
$$

where $\tilde{U} = x + y + \sum_{I_i \in \mathcal{I}} z_i \cdot P_i$ is the sum of investments in the firewall, IDS and insurance. The first term of Eq. (5) implies that the expected damage $\bar{U}$ is higher than the limit of liability, the agent will pay the excess cost. Otherwise the insurance will cover the entire cost. The indicator function in the second term is defined as: $I(B) = 0$ if $B < \infty$, which means the risk management is constrained by a finite budget B and $I(B) = 1$ if $B = \infty$, which means the risk management is without any budget constraint. Our goal is to compute the optimal assignment of the budget to maximize the agent's expected utility.

3 Experiment

We conducted an experiment to test the extent to which model predictions correspond with actual user behavior, at least in controlled settings. To do so, we developed a web-based experimental system that presents trials, resembling

incoming email messages. Participants had to classify messages as malicious or non-malicious. The experiment consisted of six sessions. At the beginning of each session, participants decided how much they wanted to invest in a firewall, an IDS and insurance. Greater investment in each of the security measures led to greater protection. The system assigned the participants randomly to one of the four experimental conditions. The conditions differed in the optimal investment in the security measures (firewall, IDS, or insurance). In three of the four conditions, the optimal investment in one of the measures was the maximum 10, and it was 0 for the two other measures. In the fourth condition, the optimal investment was 0 for all measures.

3.1 Participants

Participants were 98 engineering students (59 females and 39 males), with 24 participants in condition 1, 24 participants in condition 2, 20 participants in condition 3, and 30 participants in condition 4. Most (84 participants) performed the experiment as part of a project in a course on quantitative models of human performance, while the remaining 14 responded to requests by the experimenter to participate in the study.

3.2 Experiment Description

The game is played by 98 independent players, who are all potential victims of attacks, where the attacker is modeled by the system. The game consists of 6 sessions, with 30 trials in each session. In each trial, security attacks occur probabilistically, according to a fixed, exogenous probability $p = .3$, which determines the baseline rate of security attacks. The success or failure of an attempted attack depends on the defensive measures purchased by the player in the beginning of each session. Each session began with investment screen in which the participant could explore and eventually choose a combination of investments, consisting of investments between 0 and 10 points in each of the three security systems, from a total budget of 30 points in each session:

a An automatic system (resembling a firewall) that blocks part of the malicious events, letting all non-malicious events through. The greater the investment in the firewall, the larger the proportion of malicious components the system blocks.
b An automatic alert system (referred to as the Intrusion Detection System, IDS), which either issues or does not issue an alert that indicates a malicious component. The greater the investment in the IDS, the greater its ability to distinguish between malicious and non-malicious components (in Signal Detection terms, its sensitivity increases).
c Insurance that will compensate for some or all of the damage caused when a malicious component got through. The greater the investment in the insurance, the higher the proportion of the damage the insurance covers.

Participants could check the system quality as per the different potential investment mixtures as many times as they wanted. The quality of the systems was presented as the percentage of the malicious components that are stopped by the firewall, the *True Positive* and *False Positive* rate of the IDS and the percentage of compensation from the insurance for damage caused by malicious events. After selecting the investment mixture, the participant needed to classify 30 events per session.

Events were blocked by the firewall with some probability p (p depends on the participant's investment in the Firewall security system x). In Condition 1, when the optimal investment in the firewall was to invest 10 points $p(x) = 1.37 - e^{-1e^{-0.2x}}$, so that with the maximal investment, the firewall blocked .5 of the malicious events. In the other conditions, $p(x) = 1.9 - e^{-0.1e^{-0.3x}}$. Here the maximal investment in the firewall only blocked .105 of the malicious events.

The participant's investment in the IDS determined the system sensitivity. The larger the investment, the better was the ability to distinguish between malicious and non-malicious events. For Condition 2, in which the maximal investment in the IDS was optimal, $\lambda_s^I = 1 - e^{-4e^{-0.5x}}$. For the other conditions, $\lambda_n^I = 1 + e^{-4e^{-0.5x}}$. Figure 2 shows the probabilities P_{TP} and P_{FP} in the IDS for different investments for Condition 2 and the other conditions.

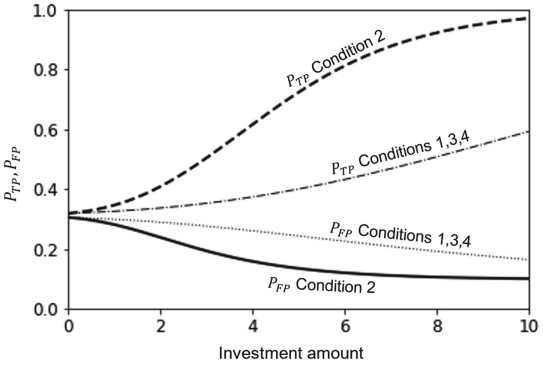

Fig. 2. P_{TP}, P_{FP} as functions of the investment in the IDS for Condition 2 and Conditions 1, 3 and 4.

If participants purchased insurance, they were compensated for some of the damage if they mistakenly classified a malicious event as non-malicious. For Condition 3, in which the optimal investment in the insurance was the maximal investment, the proportion of the damage covered by the insurance was $I(z) = 0.08x$. In the other conditions, the proportion of the damage covered by the insurance was $I(z) = 0.03x$.

The private information the participant had about an event was shown as a rectangle. The longer the rectangle, the greater the probability that the component was malicious (length was presented visually, as well as with a numerical

value). Participants classified the events by using their private knowledge (the rectangle length) the likelihood of an event being malicious, given the properties of the firewall and the IDS, and the expected damage from malicious events, given the investment in the insurance.

Classifying a malicious event as non-malicious resulted in the loss of 6 points, while correctly classifying a non-malicious event resulted in the gain of 3 points (no gain or loss of points in other cases).

After classifying 30 components, the session ended and the next session began. Participants' points were reset, and they could choose a new investment mixture and then moved on to classify 30 additional events.

4 Results

4.1 Analysis of the Investment Choices

We analyzed the investment in the three security measures in the six sessions for the four conditions with a three-way Analysis of Variance. The security measure (firewall, IDS or insurance) and the session (six sessions) were within-subject variables, and the condition was a between-subject variable. We report the significance of effects with Greenhouse-Geisser corrections for all within- subject effects. There was a significant main effect of the security measure, $F(1.995, 187.56) = 43.33, MSe = 22.11, p < .001$. The investment in the IDS was overall higher ($M = 6.675$, $SD = 2.98$) than the investment in the other measures ($M_{firewall} = 4.17$, $SD_{firewall} = 3.32; M_{insurance} = 4.31$, $SD_{insurance} = 3.40$). There was also a significant main effect of the condition, $F(3, 94) = 6.94, MSe = 38.996, p < .001$. Condition 1, in which investment in the firewall was optimal, showed more investment ($M = 5.95$, $SD = 3.05$) than Condition 2 ($M = 3.76$, $SD = 4.02$), $p < 0.001$, and Condition 4, in which the optimal strategy was not to invest at all, showed more investment ($M = 5.11$, $SD = 3.23$) than Condition 2, $p < 0.05$. Also significant were the interactions Measure X Condition, $F(5.99, 22.11) = 7.54, MSe = 22.74, p < .001$. and Measure X Session, $F(8.37, 786.85) = 28.33, MSe = 6.68, p < .001$.

To gain a better understanding of the patterns of results, we conducted separate analyses for the different security measures. In the analysis of the investment in the firewall, there was a significant difference between the conditions, $F(3, 94) = 9.52, MSe = 30.62, p < .001$. The investments in Condition 1, in which investment in the firewall was optimal, were greater ($M = 6$, $SD = 2.85$) than those in Conditions 2 ($M = 2.94$, $SD = 3.35$), $p < .001$ and Condition 3 ($M = 3.02$, $SD = 3.035$), $p < .001$ according to Tukey HSD. There was no significant effect of the session for the firewall security measure. Participants rapidly realized that it is worthwhile to invest in the firewall when the investment was indeed optimal. However, they did not reach the maximal investment. There was no evidence for learning. Thus, participants did not approach the optimal investment in the firewall (raise the investment in Condition 1 to the maximum and lower the investment in all other conditions to 0).

The results for the investment in the insurance resembled those for the investment in the firewall. There was a significant difference between the conditions, $F(3, 84) = 8.762, MSe = 30.77, p < .001$. In Condition 3, in which investment in the insurance was optimal, participants invested more ($M = 6.275$, $SD = 3.15$) than in Condition 2, ($M = 2.90$, $SD = 3.15$), $p < .001$, and Condition 4 ($M = 3.84$, $SD = 2.99$), $P < .005$. Condition 1 showed more investment ($M = 4.69$, $SD = 3.28$) than Condition 2, $p < 0.05$ according to Tukey HSD. The effect of the session was again not significant. Thus, here, too, participants recognized the condition in which maximum investment in the insurance was optimal. Here, too, there was no evidence for learning over time.

In the analysis of the investment in the IDS, there was a significant difference between the sessions, as can seen in Fig. 3, $F(3.996, 375.61) = 6.38, MSe = 7.399, p < .001$. Session 1 ($M_1 = 5.43, SD_1 = 2.58$), showed less investment than any other session ($M_2 = 7$, $SD_2 = 2.75$; $M_3 = 6.91$, $SD_3 = 2.79$; $M_4 = 7$, $SD_4 = 3.00$; $M_5 = 6.99$, $SD_5 = 3.12$; $M_6 = 6.72$, $SD_6 = 3.27$). There was no significant difference between the conditions for the IDS security measure. Thus, for the IDS, participants did not differentiate between the condition in which investments in the IDS were justified and the others. There was a change over time in the investments in IDS, but it was an overall increase in the willingness to invest in the IDS, irrespective of the effect of the investment.

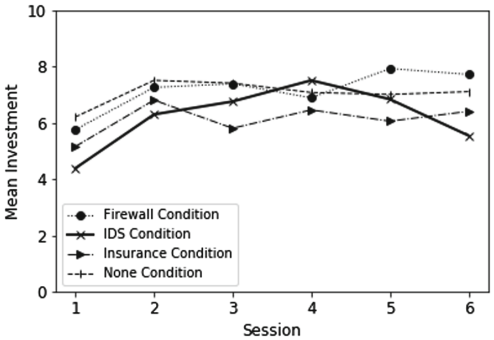

Fig. 3. IDS: mean investment for the conditions and sessions

5 Discussion

We developed a model of the optimal investment in different security measures and examined actual investment choices in three different security measures, considering the quality of the systems. The results showed that participants preferred to invest in the IDS, compared to the firewall and insurance. However, the participants were not sensitive to the quality of the IDS. People invested between 60–70% of the maximum amount in the IDS, regardless of system quality. Investments in the IDS increased from the first session to the second and then remained fairly constant. Thus, even though there was a change over time, there

was no evidence for systematic learning that moves the investments towards the optimum in the different conditions. These findings are in line with the results of previous studies that show that user choices of the settings of alerting systems are often problematic [5,14].

There was, however, some awareness of the differences in the quality of the firewall and insurance. Players invested more in these two security measures when the maximal investment was optimal, although they did not reach the optimal investments. Neither did the investment in the conditions, in which the investment in the firewall or the insurance provided no benefits, diminish. Overall, there were no significant learning effects for these two measures. Participants decided on the level of investment in them during the first session, and they maintained approximately the same level throughout the experiment.

These results indicate that people (at least in our controlled experiment) fail to make optimal decisions regarding risk taking/investment in defense systems. Therefore, an external mechanism is required to support these decisions. An additional solution is the government's regulation that specifies the properties of the security measures (e.g., the required insurance coverage).

6 Implications from Our Study

Future research should validate and expand the results in additional systems. Still, our study does show that participants do not respond adequately to properties of the security measures. They over-invest in information that is supposed to help them differentiate between threat and non-threat situations, even when this information has limited value. They do not distinguish between systems in which the information benefits them and others in which it does not.

Also, even though participants realized that some firewall and insurance conditions were better than the others, they did not adjust their responses sufficiently. They did not invest enough in the firewall or the insurance when investments could have benefited them, and they invested too much in these measures when they did not provide benefits that would have justified the investment.

In summary, our study shows that users' choices regarding the investment in security measures are problematic. Users can distinguish between better and worse investments in measures that lower the likelihood of attacks or the severity of the attack consequences. They invest more when the investment is justified, but not enough, and they invest too much when investments are not justified. When it comes to information, users invest in it, even if it is practically useless.

These findings should be considered when planning risk mitigation strategies. It may be problematic to rely on users' intuitive judgments to choose how to allocate resources to cyber security measures. Instead, it may be necessary to conduct systematic, decision-analytical evaluations of risk mitigation measures to optimally allocate the resources to cyber security measures.

Acknowledgements. The research was partly funded by the Israel Cyber Authority through the Interdisciplinary Center for Research on Cyber (ICRC) at Tel Aviv University. This research was also supported by NCR2016NCR-NCR001-0002, MOE, and NTU.

References

1. Bajcsy, R., Benzel, T., et al.: Cyber defense technology networking and evaluation. Commun. ACM **47**(3), 58–61 (2004)
2. Ben-Asher, N., Meyer, J.: The triad of risk-related behaviors (TriRB): a three-dimensional model of cyber risk taking. Hum. Factors **60**(8), 1163–1178 (2018)
3. Bissell, K., Ponemon, L.: The cost of cybercrime - unlocking the value of improved cybersecurity protection (2019). https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
4. Borgida, E., Nisbett, R.E.: The differential impact of abstract vs. concrete information on decisions 1. J. Appl. Soc. Psychol. **7**(3), 258–271 (1977)
5. Botzer, A., Meyer, J., Bak, P., Parmet, Y.: Cue threshold settings for binary categorization decisions. J. Exp. Psychol.: Appl. **16**(1), 1–15 (2010)
6. Botzer, A., Meyer, J., Borowsky, A., Gdalyahu, I., Shalom, Y.B.: Effects of cues on target search behavior. J. Exp. Psychol. **21**(1), 73–88–539 (2014)
7. Bowen, B.M., Devarajan, R., Stolfo, S.: Measuring the human factor of cyber security. In: 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 230–235. IEEE (2011)
8. Cavusoglu, H., Mishra, B., Raghunathan, S.: A model for evaluating it security investments. Commun. ACM **47**(7), 87–92 (2004)
9. Cisco: Cisco website. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. Accessed 2 May 2019
10. Lindros: CIO website. https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html. Accessed 2 May 2019
11. Marcum, J.: A statistical theory of target detection by pulsed radar. IRE Trans. Inf. Theory **6**(2), 59–267 (1960)
12. MAS: Annual report 2014/15. http://www.parliament.gov.sg/lib/sites/default/files/paperpresented/pdf/2015/. Accessed 2 May 2019
13. Meyer, J.: Conceptual issues in the study of dynamic hazard warnings. Hum. Factors **46**(2), 196–204 (2004)
14. Meyer, J., Sheridan, T.B.: The intricacies of user adjustment of system properties. Hum. Factors **59**(6), 901–910 (2017)
15. Möller, S., Ben-Asher, N., Engelbrecht, K.P., Englert, R., Meyer, J.: Modeling the behavior of users who are confronted with security mechanisms. Comput. Secur. **30**(4), 242–256 (2011)
16. Nevin, J.A.: Signal detection theory and operant behavior: a review of David M. Green and John A. Swets' signal detection theory and psychophysics1. J. Exp. Anal. Behav. **12**(3), 475 (1969)
17. Pastore, R., Scheirer, C.: Signal detection theory: considerations for general application. Psychol. Bull. **81**(12), 945 (1974)
18. Tanner Jr., W.P., Swets, J.A.: A decision-making theory of visual detection. Psychol. Rev. **61**(6), 401 (1954)
19. de Vries, J.: What drives cybersecurity investment?: organizational factors and perspectives from decision-makers. Master's thesis, System engineering, Policy Analysis and Management, Technical University Delft, Delft (2017)
20. West, R.: The psychology of security. Commun. ACM **51**(4), 34 (2008)
21. Wickens, T.D.: Elementary Signal Detection Theory. Oxford University Press, USA (2002)