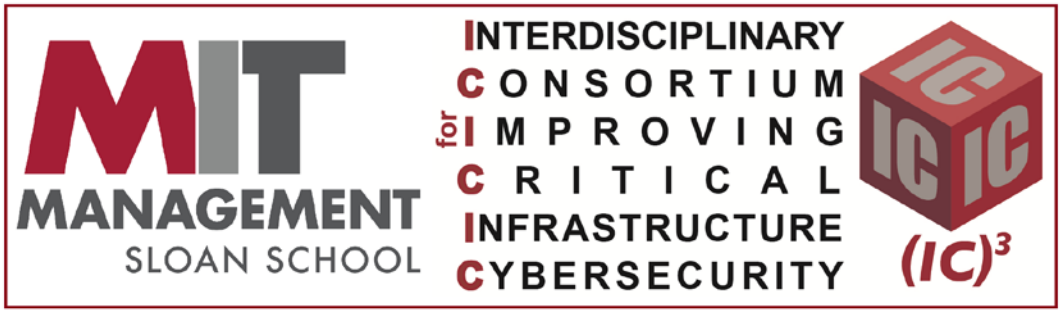


Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment

Mohammad S. Jalali
Michael Siegel
Stuart Madnick

Working Paper CISL# 2017-16

August 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment

August 2017

Mohammad S. Jalali*, Michael Siegel, and Stuart Madnick

MIT Sloan School of Management

* *Corresponding author*: jalali@mit.edu

Abstract: Despite the rise in the frequency and intensity of cyber-attacks, many organizations are still negligent in their management of cybersecurity practices. To address this shortcoming, we developed a simulation game to understand and improve how managers make investment decisions in building cybersecurity capabilities. The simulation game focuses on how managers' decisions may impact the profits of their business, considering the costs of cybersecurity capability development, the unpredictability of cyber-attacks, and potential delays in building capabilities. In an experiment with 67 individuals, we recorded and analyzed 1,479 simulation runs. We compared the performances of a group of experienced cybersecurity professionals with diverse industry backgrounds to an inexperienced control group. Both groups exhibited similar systematic errors in decision-making, indicative of erroneous heuristics when dealing with uncertainty. Experienced subjects did not understand the mechanisms of delays any better than inexperienced subjects, and in fact, performed worse in a less uncertain environment, suggesting more developed heuristics. Our findings highlight the importance of training and education for decision-makers and professionals in cybersecurity, and lay the groundwork for future research in uncovering mental biases about the complexities of cybersecurity capability development.

Keywords: Cybersecurity capability development, simulation modeling, decision making biases

1. Introduction

The aftermaths of recent major data breaches and cyber-attacks—affecting organizations from Yahoo, Target, T-Mobile, Sony Pictures, and JP Morgan to the US Democratic National Committee—reveal how critical it is for organizations to remain vigilant and act effectively in protecting against cyber incidents. In December 2016, Yahoo announced that over one billion accounts had been compromised in a recent incident [1]. Given that the estimated cost of a cyber incident is $52-$87 per compromised record [2], and that the sheer number of affected records in a data breach could be on the order of millions, if not more, the potential monetary impact of cyber-attacks is significant. In May 2017, Target agreed to pay $18.5 million in settlements and the total cost of the 2013 data breach reached $292 million [3]. Beyond the financial impact [4], a cyber-attack may, for example, cause irreparable damage to a firm in the form of corporate liability [5], a weakened competitive position, and loss of credibility [6].

In coming years, the threat posed by cyber-attacks will continue to grow as attacks become more sophisticated and organizations continue to implement innovative technologies that often, albeit inadvertently, introduce new, more subtle vulnerabilities. The Ponemon Institute posited in a 2016 study that the cost of data breaches has increased by 30% over the past three years and that there is a 26% probability that any given organization will experience a breach within the next two years [7]. Research also suggests that attackers in cyberspace are not only rational and motivated by economic incentives, but also act strategically in identifying targets and approaches [8]—"The good guys are getting better, but the bad guys are getting badder faster" [9]. Perhaps there was a time a decade ago when cybersecurity was only a matter of "if" an organization was going to be compromised, but today it has become a question of "when," and "at what level."

Despite the proliferation of cyber-attack capabilities and their potential implications, many organizations still perform poorly with respect to cybersecurity management. These companies ignore or underestimate cyber risks, or rely solely on generic off-the-shelf cybersecurity solutions. A mere 19% of chief information security officers (CISOs) are confident that their companies can effectively address a cybersecurity incident [7]. In 2016 and 2017, many American hospitals were victims of ransomware, a type of malware that blocks access to computer systems until a ransom, often in Bitcoin, is paid. In one case, the US government and the provider of the hospital's web application server, Red Hat, had even issued repeated warnings about security flaws over the course of almost 10 years [10]. Fixing the ransomware vulnerability involved installing an available update, or manually deleting two lines of software code. Despite the simplicity of the fix, the hospital did not take any action to address the security risk. In a similar incident in May 2017, the WannaCry ransomware attack targeting Windows systems affected companies worldwide, even though a patch for the exploited system vulnerabilities had been made available by Microsoft months earlier in March 2017 [11]. As data becomes more readily available and privacy concerns escalate, how can such negligent behavior regarding cybersecurity persist in organizations across the world?

To bring awareness to organizational perspectives on cybersecurity, the cybersecurity community has made efforts to intervene by involving and educating top-level managers and executives. Cybersecurity concerns affect an entire organization, not just information technology (IT) departments

or isolated response teams; therefore, the responsibility to address such issues should belong to managers at higher organizational levels. Executive commitment and support of IT in general, [12, 13] and of information security in particular, is a well-studied area [14, 15]. Research shows that commitment by top executives is essential for adoption, implementation, and assimilation of security capabilities [16-18]. Moreover, the importance of being proactive in cybersecurity capability development is well understood—it is more cost effective than taking a reactionary approach and reduces failure rates [19]. Although many executives are becoming aware of the significance of cybersecurity, several questions remain unanswered: How proactive are executives and decision-makers in building cybersecurity capabilities? And, how well do they understand the complexities of building cybersecurity capabilities?

In an attempt to answer these questions, we developed a management simulation game, and conducted an experiment with experienced professionals in cybersecurity from diverse industries and inexperienced graduate students. In our game, players decide how to invest in building cybersecurity capabilities for an anonymous company and monitor the effects of their decisions over the course of five years in the game.

Our study contributes to the literature on cybersecurity in three ways: It sheds light on the dynamics of cybersecurity capability development from an organizational perspective, examines the effects of different configurations of cybersecurity capabilities, and applies a system dynamics approach to cybersecurity. Firstly, drawing upon the strategic management and organizational science literature, we focus on the 'dynamics' of cybersecurity capability development with regards to the impact of uncertainty and delays. Secondly, the intersection of information security and decision-making gives rise to new questions on the effects of different configurations of cybersecurity capabilities in industry, which may vary due to the uncertainty of cyber risk. Researchers have studied cybersecurity investment strategies in general (e.g., see [20-22]), in addition to the more specific question of trade-offs between proactive and reactive investment strategies , e.g., [19]; however, individuals' biases and misconceptions regarding proactive and reactive investment decisions receive little attention. Our simulation game experiment allows us to analyze this aspect of cybersecurity capability investment. Thirdly, systems thinking in general and system dynamics modeling in particular are not new approaches in the area of information science and technology (e.g., see [23, 24]), yet rarely applied to cybersecurity—especially to business and management aspects of cybersecurity. Our simulation game views the problem of investment from a systematic perspective, and the underlying development uses system dynamics simulation modeling.

This paper is organized as follows: We first review relevant literature and theoretical background information leading up to our research hypotheses. Next, we present our research methodology, including the simulation game and the experimental setup, followed by experimental results, analysis, and discussion. Finally, we present implications and conclusions.

2. Theoretical background and hypotheses development

From a general organizational perspective, organizational 'capability' is a high-level routine or collection of routines [25] that delineates a firm's ability to leverage its resources [26]. In other words, it is the ability of an organization to produce a particular output [27]. From a resource-based

perspective, Bharadwaj [26] developed the concept of IT as an organizational capability. Here, we consider cybersecurity capability as an organizational capability and focus on its configuration within organizations.

Strategic management and organizational science literature shows that differences in configurations of organizational resources and capabilities explain much of the heterogeneity in organizational performance [28-30]; however, achieving optimal configurations of resources and capabilities is a complex task in which not all organizations succeed [31-33]. Similarly, configuration of cybersecurity capabilities is inextricably tied to organizational performance, and evidence shows that major variations in the configuration of cybersecurity resources exist from company to company [34].

As an example, consider two similar organizations: organization A and B. Organization A has already invested and allocated some of its resources to develop cybersecurity capabilities and as a result has well-defined plans for maintaining such capabilities. However, organization B does not have a similar perspective on cybersecurity and will only respond to cyber events in an unprepared, reactive mode. While these two different configurations of resources can explain differences in response speed and the effectiveness of responses in the wake of a cyber-attack, the key question is what drives organization A, and not organization B, to allocate its resources to preemptive measures. In other words, what differences exist between managerial perspectives in resource allocation with respect to cybersecurity?

Effective investments in IT [35, 36], and in information security in particular [22, 37-40], have long been topics of interest in both academic and industry circles. In general, by allocating resources to cybersecurity capabilities, managers can not only effectively reduce potential losses due to cyber-attacks, but also improve overall performance of their the operations [22]. It remains that the diversion of funds away from profit-making processes and assets reduces cash flow [41]; this issue is exacerbated in small and medium-sized enterprises where there is often little or no additional funding available for cybersecurity [42]. Furthermore, unlike investors who can diversify their holdings according to their appetite for risk, managers often have limited tenure in their organizations and have little choice in dealing with the risk that their company faces. Managers have to make trade-offs with regard to how they invest their resources to defend their systems [42], and it turns out that incentives drive managers to protect organizational assets in the short-term at the expense of planning for the long-term [41].

There are usually trade-offs in building alternative resources that increase the failure risk [43]. For example, organizations may focus on existing practices that have performed well in the past, ignoring emerging opportunities [44, 45], and undervaluing investments with payoffs in the long-term [46, 47]. Empirical studies provide strong support for many quality and process improvement programs [48, 49], yet firms often fail to fully realize these benefits for several reasons: First, resources are too often withdrawn from the programs before full results are observed. Second, initial enthusiasm for programs overwhelms the available training capacity, leading to a perception that the program is not effective. And third, a penchant for short-term gains overloads the system and firms are pushed into a firefighting mode of operation [50-53]. Similarly, many cybersecurity capabilities that could prove beneficial in the long run require sizable initial investments with considerable delay before benefits materialize.

While the growing bank of literature on cybersecurity discusses the above questions to a certain extent, the answers we seek are rooted in misconceptions about two aspects of complexity that have

received little attention: the uncertainty surrounding cyber incidents, and delays in building cybersecurity capabilities. We discuss these two aspects next.

2.1. Uncertainty of cyber incidents

In conventional decision-making theories, the trade-off between risk and expected return is resolved by calculating risks and choosing among risk-return combinations [54]. A rational decision-maker invests in information security if the investment yields a positive return, or if the cost of the investment is less than that of risk it eliminates. With these decisions, it is critical to have information not only about the likelihood of security incidents, but also about the impact of information security risks; however, when it comes to allocating resources to information security, difficulties in measuring the costs and benefits of information security investments cloud the vision of the rational decision-maker [55]. In addition, a consensus is rarely found among stakeholders regarding such cost-benefit analyses [56]. In risk management, it is difficult to measure the hypothetical impact of an event that is avoided [57]. Similarly, in the case of cybersecurity investment, it is difficult to estimate the impact of a hypothetical cyber incident. Further complications include a lack of historical data and effective metrics related to cyber-attacks [58], a lack of knowledge about the type and range of uncertainties, a high level of complexity, the nature of connections between entities, and little opportunity to predict future events [59]. Consequently, managers often make decisions based on their experience, judgment, and their best knowledge concerning the likelihood of uncertain events, such as cyber incidents [58].

While a manager's perception of risk is driven by his or her organizational and information system environment, as well as individual characteristics [60], research shows that humans in general do not have a strong intuition when it comes to low-probability, high-consequence scenarios, like cyber-attacks. Intuitive assessment of probability is often based on perceptual quantities, such as distance, scale, or size. Consider an example borrowed from behavioral economics: The more sharply one can see an object, the closer it appears [61], but if visibility is poor, people tend to underestimate the distance between themselves and the object.

At the organizational level, firms typically perform intensive technical analyses to determine how to allocate resources, but in the case of cybersecurity, there are often little to no performance metrics available, leading to uninformed expectations of cyber risk [62]. Because quantitative metrics for cyber risk are so sparse, companies often do not consider the typical return-on-investment values to guide investment in cybersecurity [63]. Indeed, using an unfamiliar metric to value cybersecurity investment may lead to further discounting of expectations of cyber risk.

The uncertain nature and severity of cyber threats, compounded with frequent shifts in technology acquisition and the introduction of new vulnerabilities makes it difficult for decision-makers to allocate resources for investment in cybersecurity capabilities [64]. The growing presence of cyber threats has resulted in an environment that has produced a large stream of information that focuses on technical defenses, but neglects the economics of cybersecurity investment [65]. If a company does not experience any cyber-attacks—more precisely, if it does not detect any cyber-attacks—there is little motivation to invest in security. For this reason, many managers often do not envision cyber risk properly, hence, it is not surprising to observe significant gaps between managers' perceptions, and the actual state of the cybersecurity of their organizations [66]. As a result, they may underestimate the

frequency at which incidents could occur, and the time it takes for cybersecurity capabilities to become active in preventing, detecting, and responding to an incident.

We suspect that in settings with high levels of uncertainty, such as in cybersecurity, general managerial experience will not benefit a player in the simulation game. Thus, our first hypothesis (H1) is as follows:

> *H1: For building cybersecurity capabilities, players with managerial experience in cybersecurity do not perform better than inexperienced players when faced with uncertainty.*

2.2. Complex systems and delays in building cybersecurity capabilities

A complex system includes a web of interconnected components, among which there are potential delays. Regardless of the complexity of a system, a manager's problem solving method is often reactionary and event-oriented [67]; however, the use of event-oriented decision making frameworks (e.g., situation and goals → problem → decisions → results) leads to a failure to understand the connections among components and potential delays between cause and effect. Delays between applying a decision and its effect create instability, increasing the tendency of a system to oscillate, and pushing managers to attempt to reduce this perceived time gap long after proper corrective actions have been taken to restore the system to equilibrium [67]. Hence, a lack of understanding of the delays inherent in a system can lead to ineffective decision-making.

Even simple systems are not immune to this problem, as time delays and feedback loops between causes and effects can create complicated outcomes that are hard to anticipate [68]. Indeed, even highly educated and experienced individuals perform poorly when making decisions in such dynamic and complex settings—see [69-72] for examples in various research settings. Despite these findings in other settings, practitioners in information security may believe that experienced managers understand the impact of delays better than inexperienced individuals, because of their extensive experience in industry.

Like other complex systems, cybersecurity systems include potential delays. For instance, the time it takes to develop and build cybersecurity capabilities is a major source of delays, often taking years, as well as the delay in training employees. Human factors play a crucial role in cybersecurity [73], and recent analyses show that employees are often the weakest link in an organization with regard to cybersecurity [74]. As a result, organizations are urged to consider investing in cybersecurity training as a top priority [75], and to encourage protection-motivated behaviors [76, 77]. These recommendations mean nothing if organizations fail to understand the impacts of delays and fall into the trap of short-termism. Considering the delays required for the adoption of, or transition to new technologies, and for providing necessary cybersecurity training to employees, organizations may not see a return from cybersecurity training for several years.

In a reactive organization where managers start investing in the development of cybersecurity capabilities only after detecting an attack, the organization's computer-based information systems will not properly recover in time and remain vulnerable to other attacks in the meantime. While the delay between cybersecurity decisions and their ultimate effects seems simple in theory—with which experienced managers would be familiar—the possession of such necessary intuition among managers is far from adequate. Thus, our second hypothesis (H2) is as follows:

H2: In building cybersecurity capabilities, players with managerial experience in cybersecurity do not understand the effects of delays better than inexperienced players.

3. Methods

We developed a management simulation game to study individuals' decisions when building cybersecurity capabilities in an experimental setting. In this section, we describe the simulation game and present the experimental setup.

3.1. Why a simulation game

Simulations are widely used to train professionals in a variety of settings. For example, pilots are required to have a certain number of hours logged in flight simulators before flying a jet, and similarly, managers should have appropriate training before assuming leadership positions in complex organizational environments [78]. Management flight simulators are interactive tools that provide a virtual environment for decision-makers. Unlike in the real world, where a bad choice may result in the failure of a business, simulations allow managers to practice decision-making skills without fear of real consequences outside of the game.

Management flight simulators are potentially helpful for observing the long-term consequences of a decision or series of decisions. Similar applications have been developed in other fields, such as the Climate Interactive (C-ROADS) simulator in climate change policy [79], People Express in strategic management [80], and ReThink Health in health policy [81, 82]. These simulators are developed based on simulation models that describe the complexity of managerial phenomena while remaining a simplification of reality.

In addition to providing a tool to conduct this study, our simulation game will allow managers to experience the complexities of allocating resources for building cybersecurity capabilities. The game focuses on how a manager's decisions may impact his or her business' profits, given the costs of capability development, potential delays in building capabilities, and the unpredictability of cyber-attacks. Players can interactively learn how to respond to unique high-risk situations.

3.2. Cybersecurity simulation game

In this section, we describe cybersecurity capabilities and then present the simulation game and the setup of the experiment.

3.2.1. Cybersecurity capabilities at the core

As has been discussed, the game focuses on building cybersecurity capabilities. Interventions to build such capabilities typically include improvements to technology already in place, in addition to the purchase of new technology, talent acquisition, and training, among other activities. For simplicity in the simulation, rather than the five categories of the National Institute of Standards and Technology (NIST) cybersecurity framework [83]—identify, protect, detect, response, and recover—we split cybersecurity capabilities into three general categories: prevention, detection, and response capabilities. Prevention capabilities help prevent computer-based information systems from being compromised by cyber-attacks. Detection capabilities help detect systems that are at risk of, or presently under attack. Response capabilities help fix vulnerabilities and mitigate the damage done by an attack.

3.2.2. Simulation model in the game

The game is developed based on a system dynamics simulation model. The model includes three main entities: computer-based information systems, cybersecurity capabilities, and cyber incidents. Computer-based information systems are divided into four groups (visualized in the "Eco-system of computerized systems" section in Figure 1): 1) "systems not at risk" (systems with no known vulnerabilities), 2) "systems at risk" (systems with a vulnerability, such as an unpatched), 3) "affected systems" (an attacker has taken advantage of the vulnerability), and 4) "affected systems that are detected" (the attack has been discovered). We discuss them in more details below.

Model structure and formulation

Cybersecurity capabilities are divided into three groups: prevention, detection, and response capabilities. Players make decisions on the percentage amount of resources to allocate towards building these capabilities, and how to divide the allocation of those resources between those capabilities. Figure 1 presents the general structure of the simulation model, with details to follow.

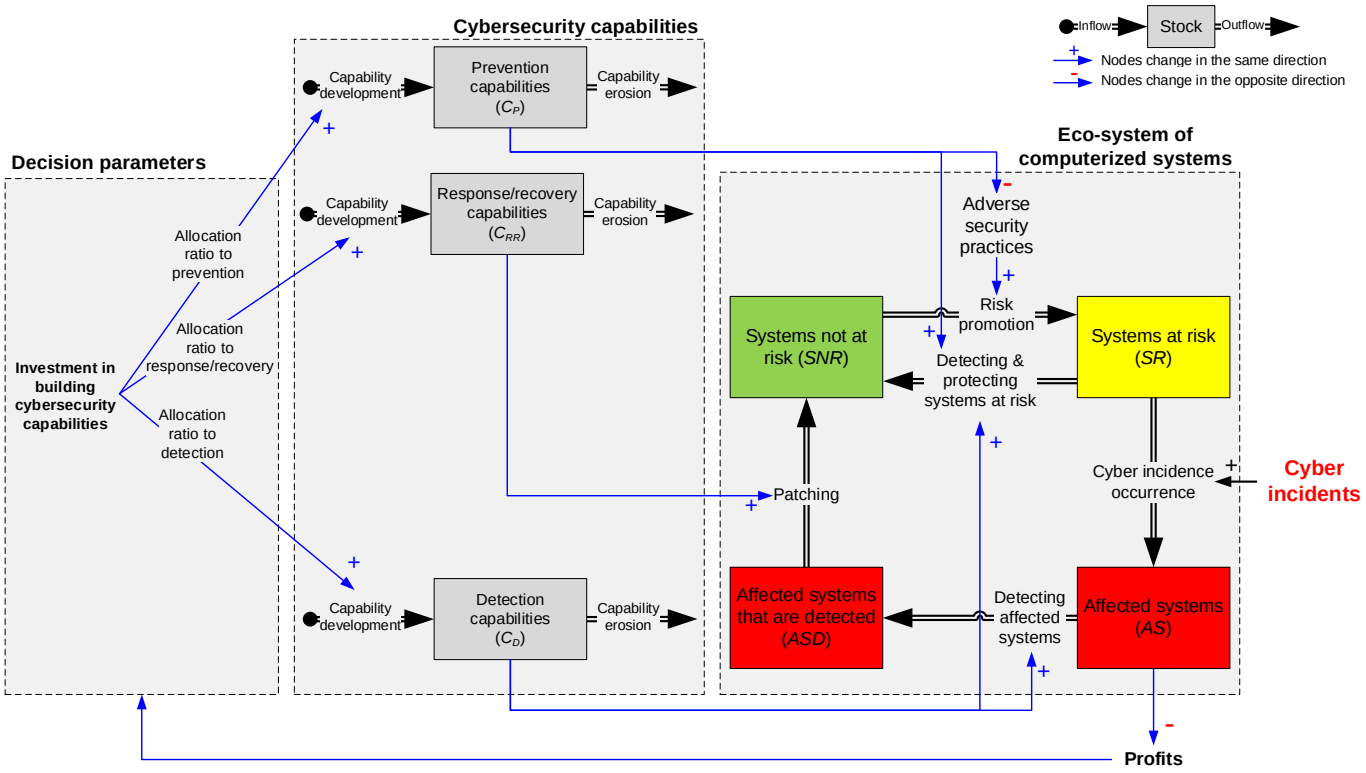


Figure 1: The general structure of the simulation model used in the game

Players decide what percentage of their resources to spend on cybersecurity and how to distribute those resources among the three capability categories—see "Decision parameters" in Figure 1. Following the basics of organizational capability development [84], each category of capabilities (C) is affected by the inflow "Capability development", $I(t)$, and the outflow of "Capability erosion", $O(t)$. Hence, the speed of change of the capability is $\frac{dC(t)}{dt} = I(t) - O(t)$, where t is the simulation time. Each

capability builds according to the decision parameters set by players, i.e., how much of available resources are allocated to each capability; however, each capability erodes gradually over time. The erosion takes place at the average life of capability (a), hence: $O(t) = \frac{C(t)}{a}$. Similar formulations are used in other settings—see [84-86].

We assume that there are multiple computer-based information systems in an organization and that all systems are initially in the "Systems not at risk" (*SNR*) group. As inadequate security practices persist, they may be moved to "Systems at Risk", *SR*. The speed at which this occurs is determined by the "Risk Promotion" rate. Prevention capabilities combat ineffective security practices and therefore decrease the flow of systems from not-at-risk to at-risk. Risk promotion is calculated as $\frac{SNR(t).ASP(t)}{b_{PR}}$, where *ASP* (adverse security practices) is calculated as $\frac{1}{C_P(t)+1}$, with C_P representing prevention capabilities, and b_{PR} representing the average duration to promote risk. Detection capabilities help detect cyber threats and limit the size of *SR* so that systems can be moved back to *SNR*. The flow from *SR* to *SNR* is calculated as $\frac{SR(t)\frac{1}{C_D(t)+C_P(t)+1}}{b_{DSR}}$, where $C_D(t)$ is detection capabilities at time t, and b_{DSR} is the average duration to detect *SR*.

Systems at risk are vulnerable and can be affected at the onset of a cyber-attack. Once affected, a system is moved to "Affected systems", *AS*. The rate of "Cyber incident occurrence", *CIO*, is calculated as $CIO(t) = SR(t).CI(t)$, where $CI(t)$ is an exogenous set of cyber incidents over the course of the simulation, which we will discuss in this section. Affected systems remain in the organization until they are detected, which depends on the adoption of detection capabilities. Once detected, systems are moved to "Affected systems that are detected", *ASD*, at a rate of $\frac{AS(t)\frac{1}{C_D(t)+1}}{b_{DAS}}$, where b_{DAS} is the average duration to detect that a system is in *AS*. Eventually, if proper response and recovery capabilities are in place, a system in *ASD* can be recovered, and moved back to *SNR*. The rate at which this occurs is the patching rate, determined by $\frac{ASD(t)\frac{1}{C_{RR}(t)+1}}{b_R}$, where $C_{RR}(t)$ represents an organization's response and recovery capabilities at time t, and b_R is the average duration of the process of patching a system.

It is assumed that affected systems have the potential to decrease profits. We have selected profit as the main measure of performance in the game, because monetary gains and losses are tangible and intuitive to understand. In general, the impact of cybersecurity incidents are manifested in two forms: cash flow losses and reputation damage [87]. Ultimately, both forms are translated into dollar values and we consider profits as the relevant measure. Given that organizational managers, particularly those sitting on boards or in executive roles, are typically focused on profits, it not only helps us simplify and communicate the goal of the game during experiments, but also helps players better monitor their performance and understand the effects of their decisions in the simulation.

In practice, the decision to commit to cybersecurity investment results in immediate costs associated to adoption of new technologies, including usage, and learning and switching costs, among others [88]; however, the benefits of possessing cybersecurity capabilities is harder to see than its

immediate costs. Resources spent on cybersecurity investments go towards mitigating the risk of cyber incidents, which may never occur [89]. Due to the nature of cybersecurity investment, it is difficult for managers to estimate the value of cybersecurity capabilities without readily available empirical evidence.

We consider the trade-offs between two major effects of allocating resources to building cybersecurity capabilities: 1) Reduced profits as building cybersecurity capabilities is an expense; 2) Possibility of protecting the organization from costly cyber-attacks. Therefore, organizational resources, R, are either spent on making profits, R_P, or developing cybersecurity capabilities, R_C, where $R = R_P + R_C$. Hence, profits, P, are calculated as $P = \alpha \cdot R_P \cdot (1 + \xi)$. The impact of affected systems on profit, α, is assumed to follow the non-linear functional form $\alpha = 1 - (AS/T)^{1/2}$, where T is the total number of computer-based information systems in the organization. In our example, $T = 100$. Profit is also subject to random shock ξ—this exogenous shock is a pink-noise distributed normally according to $\xi \sim N(0.\sigma_\xi^2)$ [90], assuming the correlation time to be three months, and $\sigma_\xi = 0.1$.

As the players in the game can monitor profits over time and adjust their decisions accordingly, a feedback link is drawn from profits back to the decision parameters in Figure 1. The goal of the game is to maximize profits (specifically, accumulated profits over the course of a simulation run) by most efficiently allocating resources. Each simulation run takes 60 months. The trade-off between profits and protection poses a challenge, and adds to the complexity of the decision-making process already muddied by the uncertainties and delays discussed in Section 2.

Cyber incident patterns

Five cyber incidents with different levels of impact occur in each simulation run (the higher the impact of the attack, the more influence on profit reduction). To keep the game simple, it is assumed that all attacks are considered external attacks, in that they originate outside of the victim organization's network, and are not categorized by type, such as a phishing attack or a network-traveling worm. While we acknowledge that the risk of an insider attack is significant in reality [91, 92], the simplifications we apply do not impact the relevance of our results, since most successful cyber-attacks result in data loss or operational disruptions regardless of their nature. Figure 2-a shows a pattern of five cyber incidents (in Section 3.2.3, we will discuss how the pattern of the five attacks changes in the game), and Figure 2-b presents how the string of cyber-attacks affects profits (compare blue and red lines).

In modeling complex systems, having a detailed and complicated model does not always translate to a more realistic simulation [93]. The simplicity of our model helps us better explain the behavior of players based on its dynamics. It also allows managers from different industry sectors to better engage with the model by relating it to their own organizations.

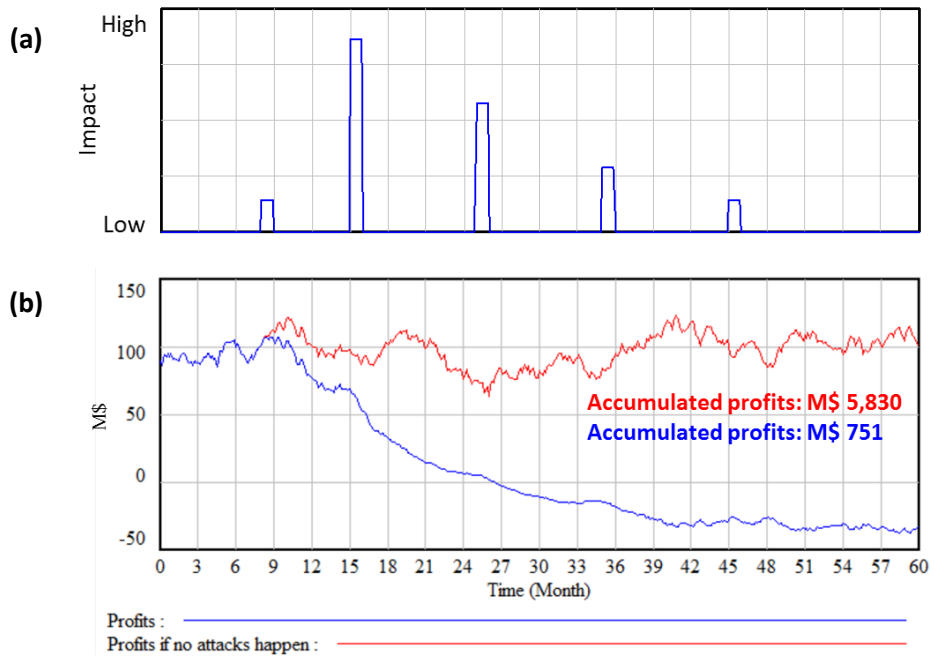


Figure 2: (a) One possible pattern of five attacks over the course of 60 months in the simulation, (b) Comparison of two simulations with (blue) and without (red) the impact of cyber-attacks.

The only difference between the two graphs in b is the occurrence of cyber-attacks, and in neither simulation is any investment made in cybersecurity capability development, so any difference in profits is directly related to the cyber-attacks shown in (a).

3.2.3. How the game works

The game runs online in an interactive environment where players have a decision parameter for each of the three types of capabilities: prevention, detection, and response. Players can adjust the value of the parameters representing the percentage of resources to allocate to each capability and when to allocate resources to each capability. Players implement their allocation strategy, advance the simulation for 12 months, monitor changes in profit and have the option to modify their allocation strategy for the next year, and advance another 12 months until 60 months, five trials, have elapsed. Each decision parameter allows the player to invest 0% to 5%, an arbitrarily set range of the IT budget, in a specific cybersecurity capability. The profit graph and accumulated profits, in millions of dollars, are shown on the same screen and they are updated any time players advance the simulation. Figure 3 shows a screenshot of the online interface of the simulation game.

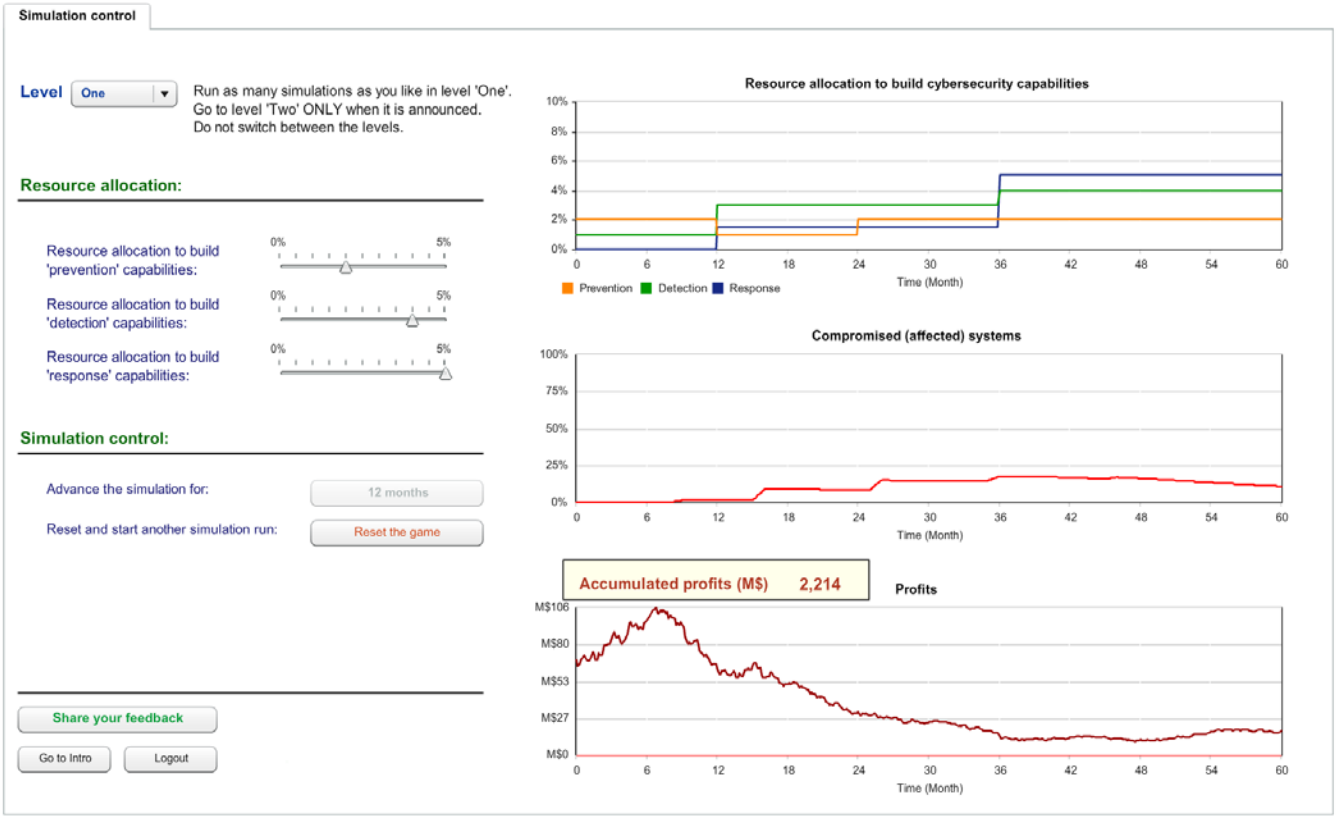


Figure 3: Screenshot of the online simulation game

Two levels of the game

The game runs in two levels. In level one (deterministic), there are five cyber-attacks with fixed impacts and at fixed times for all players. In level two (non-deterministic), five cyber-attacks happen at random times with random impacts following a uniform probability distribution. All other factors remain the same between the two levels. In the interest of fairness, the total impact of the five random attacks in level two is controlled to be equal for all players, and is also equal to the total impact of the five fixed attacks in level one.

Since differences in accumulated profit among players in level one can come only from differences in resource allocation, we expect that attentive players can learn how to maximize their profits after several runs; players can repeat simulations to learn about the optimal mix of investment parameters. In level two, on the other hand, unpredictability of attacks means that players face greater uncertainty when making decisions.

3.3. Experimental setup

The goal of this experiment was to compare the performance of an experienced group to that of an inexperienced group in both a deterministic and non-deterministic setting. We discuss the setup of the experiment below.

3.3.1 Subjects

Players were divided into two groups: the experienced (experimental) group, and the inexperienced (control) group. The experiment group included participants at a cybersecurity conference in Cambridge, Massachusetts, and totaled 38 professionals, with an average of 15 years of experience in IT and cybersecurity in a variety of industries. The control group included 29 Masters students in a general course about information technology. The experiment was conducted at the beginning of the semester so that any class materials would have minimal effect on the performance of the students, none of whom had had any prior experience in IT or cybersecurity.

3.3.2 Experiment methods

The two groups of players were tested separately. In each case, subjects played the simulation game in the same room at the same time. To avoid social influences [94], players were not allowed to talk to each other or reveal their results at any time during the game. They were given necessary background information prior to the start of the experiment in a short presentation about the three available capabilities and watched an example play-through. They were also told that the goal of the game was to maximize accumulated profit after a 5-year period and that the person with the highest profit would be awarded at the end of the game. It was made clear that no cybersecurity capabilities were already in place at the beginning of the game. Prior to playing the game, players also had the opportunity to run the simulation themselves in a practice mode and could clarify any questions they had about the game.

Subjects first played level one for ten minutes, then played level two for another ten minutes. During each ten-minute session, subjects could run the simulation as many times as they wanted. Players were not made aware of the difference between the two levels until the results of the experiment were presented at the end of the game.

4. Results

In each individual simulation run, we collected longitudinal data of the three investment decision variables (prevention, detection, and response) as well as profit data. We also collected accumulated profits at the end of each full run (after month 60) to measure individuals' performance. In the experiment and control groups, 14% and 10% of the runs were incomplete, respectively (i.e., the player left the simulation run before getting to the last month), and were thus excluded from the analysis. Table 1 presents the summary of the data included in our analysis.

Table 1: Data summary

Group	Number of players	Experience in IT or cybersecurity (years)	Number of individual runs		Median of the number of runs per player	
			Level one	Level two	Level one	Level two
Experienced	38	15	431	361	9	8.5
Inexperienced	29	0	342	345	12	12

In the following sections, we first review two individual runs as examples of proactive and reactive runs. We then present a comparison between the results of the control group and the experiment group and highlight key findings. We discuss conclusions in Section 5.

4.1. Proactive vs reactive

Figure 4 shows a proactive run and Figure 5 shows a reactive run. The trade-off discussed in Section 3.2.2 can be seen in these two figures. When proactive players start investing in capability development they make noticeably less profit than the reactive players in the early stages of the game; however, once cyber-attacks begin to occur, proactive players perform much better over the rest of the simulation.

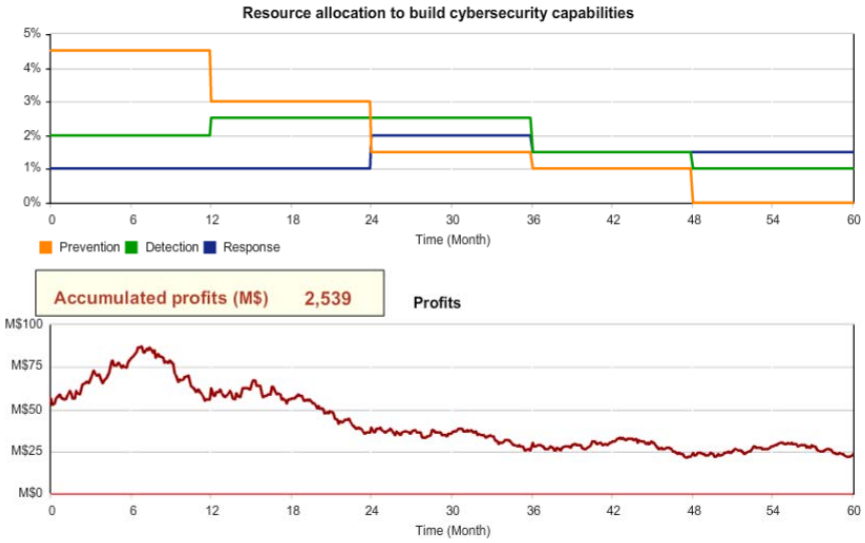


Figure 4: An example of a proactive simulation run

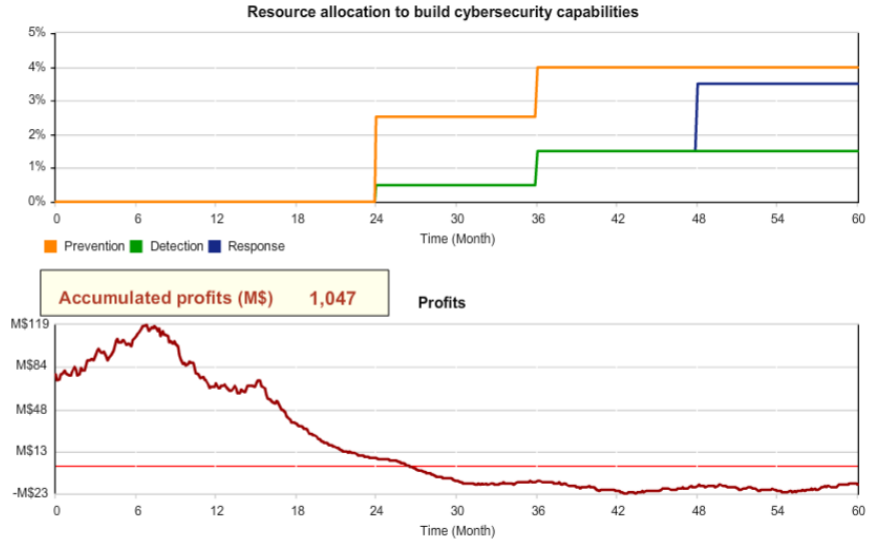


Figure 5: An example of a reactive simulation run

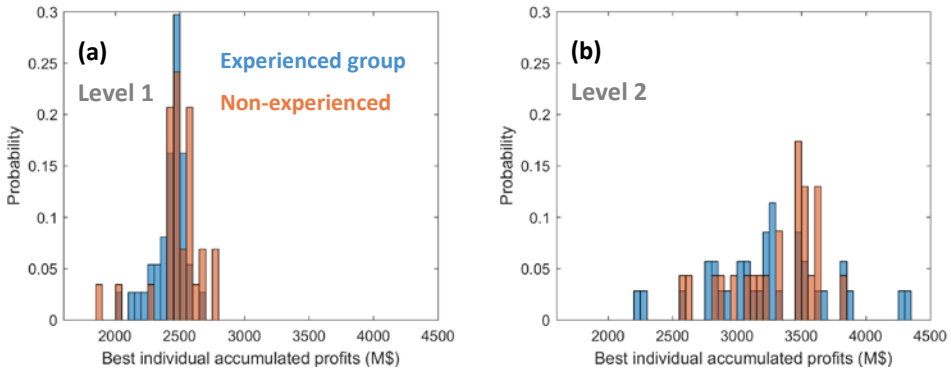
4.2. Hypothesis testing, comparison of the group results

Figure 6 shows the normalized distributions of subjects' best performances for the two levels of the game. Both experienced and inexperienced groups displayed large variations in performance in levels one and two; however, this variation is almost twice as large in level two as it is in level one. Given that the pattern of the five cyber-attacks is fixed in level one, there exists an optimal set of values of the three decision parameters to maximize accumulated profits. Consequently, the distribution is skewed left for the poor performances, while some players are clustered close to a profit of M$2,500 on the right extreme of the distribution, indicating the maximum accumulated profit. In level two, the variability in performance increases since attacks occur randomly. Figure 6-b shows the distribution of performances in level two. It should be noted that the maximum accumulated profits in level two can be higher or lower than those of level one, due to the randomness of cyber-attack occurrence. For instance, if the major attack happened at the end of a simulation run (e.g., month 55), the accumulated profits would be already higher than that in level one when the major attack happened at month 15 (see Figure 2-a).

First, we test H1 – that under high uncertainty, the experienced players do not make better decisions to develop cybersecurity capabilities than the inexperienced players. Comparing the means of the distributions in level two (the level with random cyber-attacks) using the t-test, we find that no statistically significant difference exists at the 5% significance level. Hence, we cannot reject the null hypothesis H1.

Next, we test H2 – that the experienced players do not understand the effects of delays in building cybersecurity capabilities better than inexperienced players. In other words, players with managerial experience in cybersecurity do not perform more proactively than inexperienced players. To test H2, we analyzed whether experienced players performed better in level one than inexperienced players, because only proactive investment leads to better performance in level one. We would expect experienced players to perform better than inexperienced players; however, comparing the means of the distributions using the t-test reveals that no difference exists at the 5% significance level. Therefore, we cannot reject the null hypothesis H2.

Given the interesting mixed results for experienced players' performance in level one, we next analyzed the effect of iterative learning (i.e., the effect of running a sequence of simulation runs on individuals' performance).



	mean	SD
Experienced group	2,422	133
Non-experienced group	2,484	188

	mean	SD
Experienced group	3,248	471
Non-experienced group	3,299	341

Figure 6: Distributions of best individuals' performances in level one (a) and level two (b)

4.3. Effect of players' iterative learning on their performance

Figure 7 and Table 2 present the correlations between the number of simulation runs a player made in the 10 minutes of each level and the score of their best performances. The correlations reveal whether conducting more runs helped players perform better in the game. Significantly positive correlations are observed for all groups except for the inexperienced group in level one.

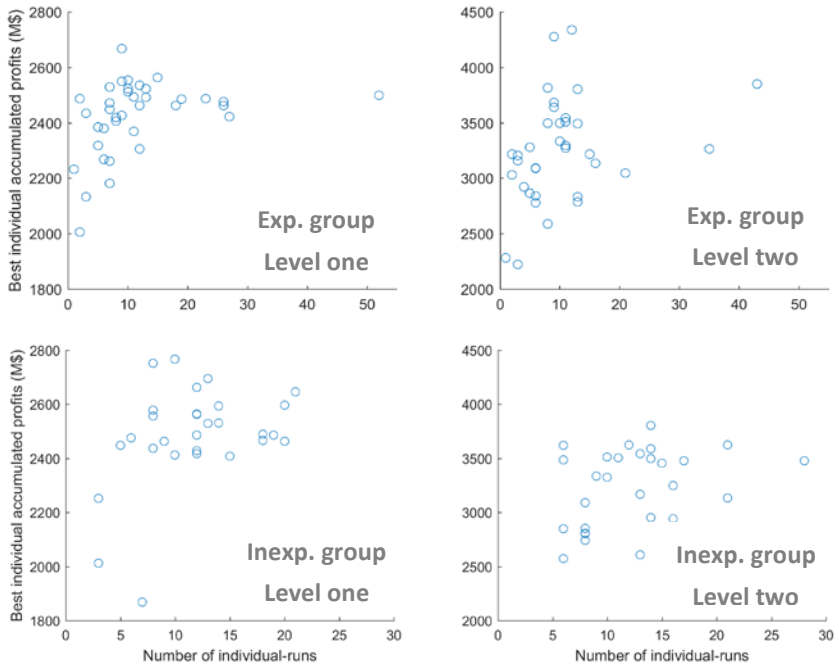


Figure 7: Relationships between the number of runs by an individual and that individual's best performance

Table 2: Correlation between the number of runs and maximizing accumulated profits

Group	Level one	Level two

	Correlation	p-value	Correlation	p-value
Experienced	0.35	0.03	0.32	0.05
Inexperienced	0.39	0.36	0.34	0.07

Here we analyze the performance of players in each level of the game. Figure 8 and Figure 9 show the variation of players' performance (Y axis; accumulative profit) through the sequence of their runs (X axis; the number of runs for the respective player) in level one and level two, respectively.

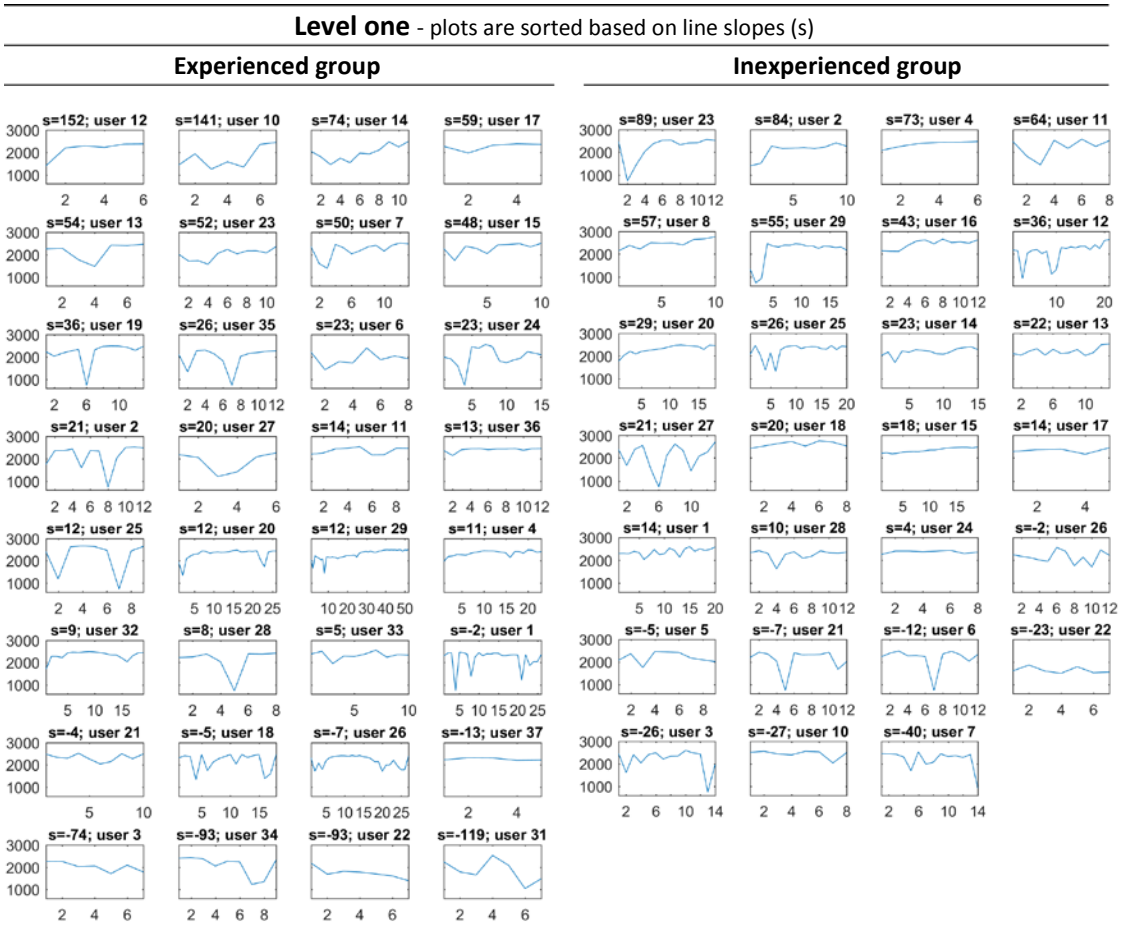


Figure 8: Learning curves of individuals in level one.

For each group, plots are sorted based on their linear slopes (s). The Y-axis represents accumulated profits. The X-axis represents the run number for each respective user. User IDs are unique numbers for players.

The graphs in Figure 8 and Figure 9 are sorted by linear slope in descending order, so that the graph in the top left-hand corner corresponds to the player who has shown the most improvement in accumulating profits over the course of his or her runs. For instance, in Figure 8, the top-left person in the experienced group (user 12) has the highest linear slope (s=152), which means the player improved his or her performance over the six runs in level one.

Considering the linear slope of a player's performances allows us to observe all of their run data and observe their learning process. For the following analysis we only considered users who played at least five rounds in a level.

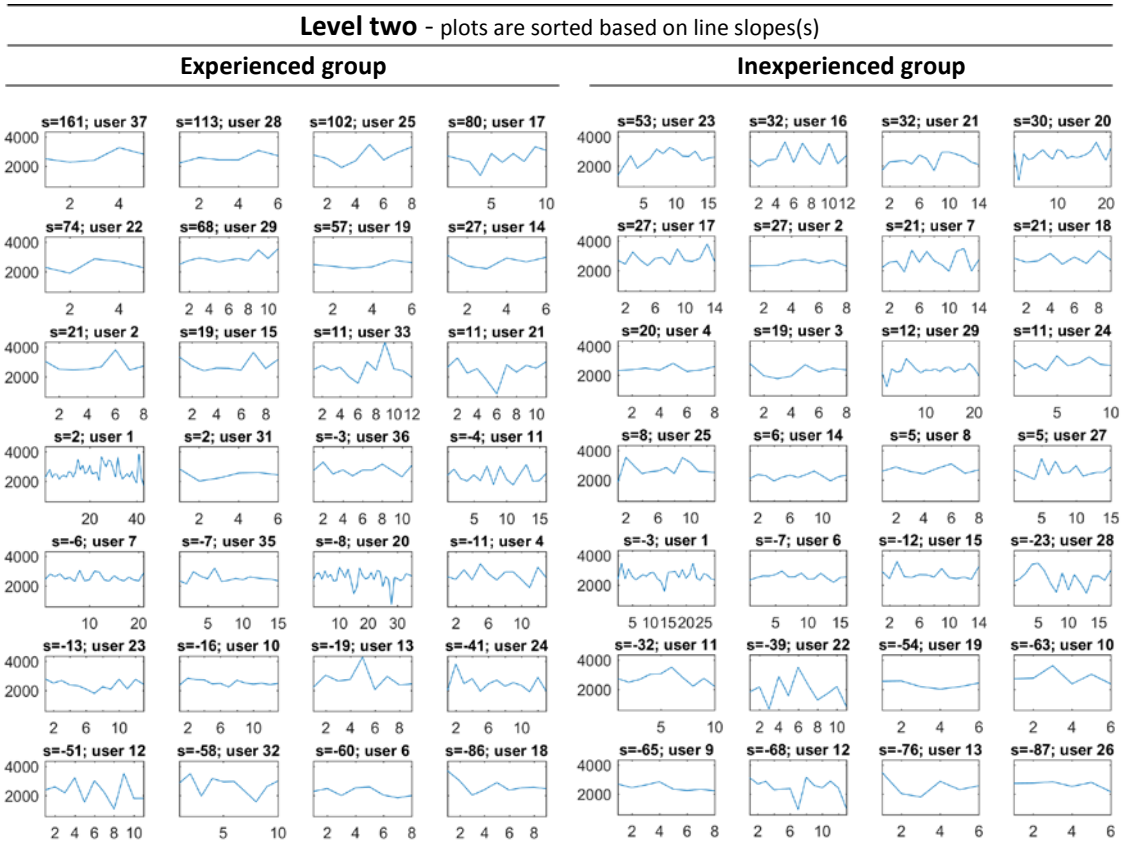


Figure 9: Learning curves of individuals in level two.

To interpret the results presented in Figure 8 and Figure 9, we sorted the users based on their linear slopes and analyzed how their ranks changed from level one to level two. Figure 10 presents this analysis. The line connecting the user ID from level one to level two shows the change in ranking between the levels. A dark red line indicates a large decrease in ranking, while a dark green line indicates a large rise in ranking.

Surprisingly, among the experienced group (the left side of Figure 10), the users who had the highest performance slope in level one performed among the worst in level two, while the users who performed poorly in level one were the better performers in level two. The top players in level one learned the game and were successful in tweaking their investment strategies to increase accumulated profits when confronted with the same fixed cyber-attacks; however, the strategies they had developed did not translate effectively to the random environment of level two, and some even performed more poorly than other players who had not performed as well in level one. This pattern is not observed in the inexperienced group (the right side of Figure 10) where the ranking of players seems to change more arbitrarily[1]. We discuss this observation further in the following section.

[1] For instance, among the experienced group, the top six experienced individuals in level one had an average of 56% decrease in ranking in level two; however, among the inexperienced group, the top six individuals in level one had an average of 22% decrease in ranking in level two.

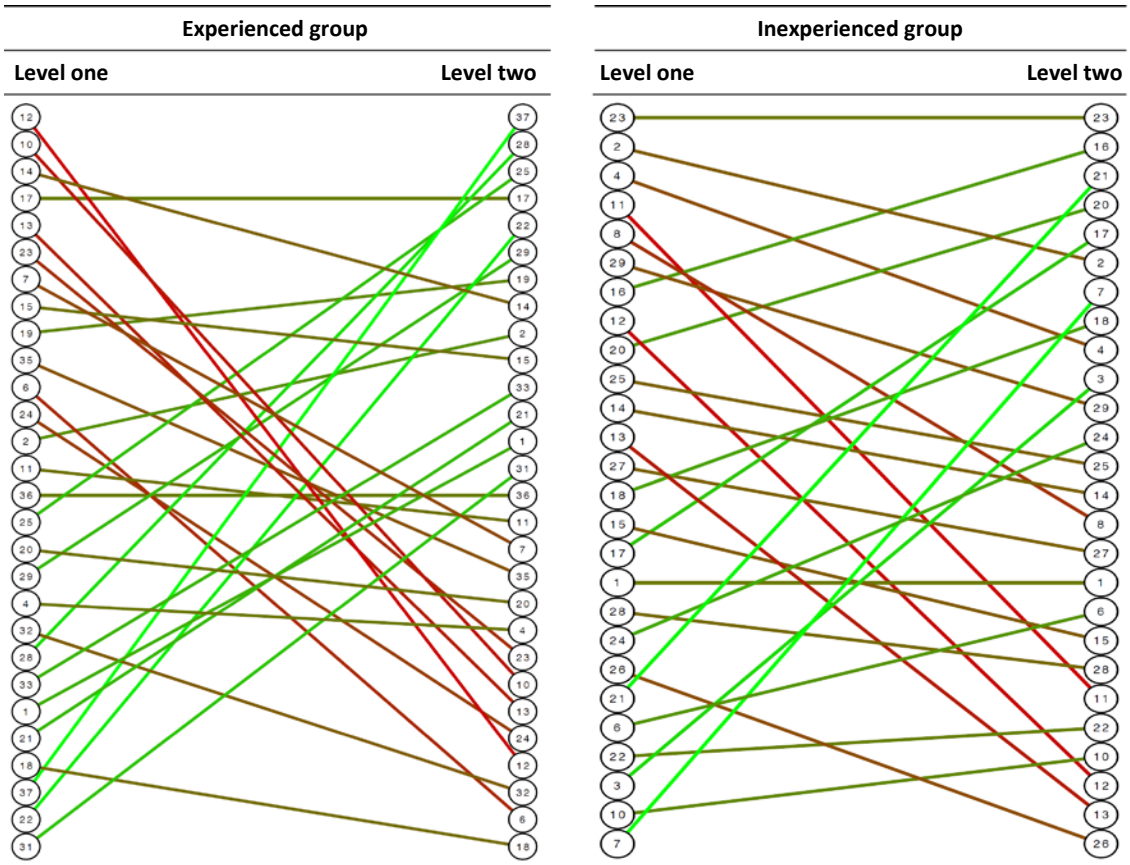


Figure 10: Mapping ranked users based on their learning slopes.

5. Discussions and conclusions

Using our simulation, we studied how players understood two fundamental aspects of complexity in cybersecurity: delays in response when building cybersecurity capabilities, and uncertainties in predicting cyber events. In this section, we will discuss these in more detail.

5.1. Analysis of experimental results

We have focused on understanding the complexities of building cybersecurity capabilities from a manager's perspective. In general, there are two properties of building cybersecurity capabilities that contribute to the difficulty of making informed decisions regarding cyber policy in an organization:

- The trade-off between allocating resources to profitable activities versus investing in cybersecurity capabilities, with the perceived payoff for the latter being affected by the delay between their development and reaching full functionality.
- The uncertainty surrounding the occurrence of cyber-events, as shown in the differences in results from the two levels of the simulation game.

We note that the main mechanisms of our game are based on general capability development dynamics not limited to cybersecurity. The insight from this study of the importance of acting proactively can be applied in other settings as well, but it remains that the organizational aspect of cybersecurity, and particularly the development of cybersecurity capabilities, has not received adequate

attention. Being proactive in building cybersecurity capabilities is critical to the success of an organization, but many experienced professionals perform poorly in this regard.

Neither experienced players nor inexperienced players showed performance differences in level two, and interestingly, experienced players performed worse than inexperienced players in level one. One possible interpretation for this poor performance is that the tightly controlled environment of level one, in which cyber-attacks happened at regular intervals and could be anticipated in repeated simulation runs, was far removed from the reality that the experienced players had experienced over their average 15 years in the field. This interpretation suggests deeply entrenched decision-making heuristics, reinforced over years of experience, and is supported directionally by our analysis of learning curves in the experienced group. Experienced players who performed well in level one did not perform well in level two, and vice versa, suggesting that their strategies did not adapt to the environment in which they were found themselves. Inexperienced players, on the other hand, showed much more dynamism in adapting to repeated runs and the changing environment between levels one and two. To support this interpretation, we next discuss common biases in managerial decision-making.

5.2. Biases in decision-making heuristics

Behavioral economics research shows that managers rely on a set of heuristics to make decisions in situations with uncertainty, and that these heuristics can potentially cause systematic errors. This phenomenon has received little attention in cybersecurity research, which is concerning, as a manager's biased assessment of cyber risk could hamper an organization's ability to respond to cyberattacks. Here we discuss two major heuristics: availability and representativeness.

Availability refers to how readily examples come to an individual's mind [95]. People assess the likelihood of risks by considering past experiences. For example, if accidents or natural catastrophes have not occurred to them in the past, people are less likely to buy insurance. Similarly, if managers have not experienced—or are not aware of—any major cyber-attacks that have affected their own organizations, they are less likely to take cyber risk seriously. Thus, the probability of cyber events occurring, given that cyber events may not be visible, is estimated to be lower than it is in actuality. The availability heuristic can also help explain why many organizations do not purchase cyber insurance until after a major cyber incident.

The second heuristic is representativeness [95]. Representativeness describes how a certain event that shares similar characteristics with another set of events is often grouped together with the other events. The fact that something is more representative does not make it more likely. Thus, individuals relying too heavily on representativeness to make judgments are liable to make a decision for the wrong reasons [96].

Representativeness can result in serious misconceptions, especially in situations involving randomness and sequences of random events. If a person flips a fair coin five times and gets head every time, they may find it difficult to believe that the coin is indeed fair. However, if they flip the coin many times (e.g., 100 times or more), they will observe that the sequence is truly random [95]. Making decisions about uncertain cyber events is subject to this same type of error. Managers may believe that cyber events are not random and will likely look for patterns informed by past events to confront

uncertainty. Using availability and representativeness heuristics together increases the chance of making the wrong decision in an uncertain world.

In addition to these two heuristics, individuals are also often overconfident in their decision-making abilities, and highly-educated, experienced managers are no exception [95]. A person's optimism can similarly cause them to overestimate the immunity of their organization to cyber-attacks, leading to failure to take sensible preventative actions. Furthermore, research shows that people tend to not make changes even when changes are in their own interests [95]. Consider a manager who already has a biased estimation of uncertainty due to availability and representativeness heuristics. Because that manager is already successful, he or she does not necessarily feel the need to deviate from a working business model and invest more in cybersecurity capability development at the cost of losing some productive resources. This is not to say that we do not recommend hiring experienced managers, but we conclude that management experience alone does not help when making decisions related to cybersecurity, and that targeted training that challenges fixed mindsets is needed for decision-makers when it comes to cybersecurity.

5.3. Limitations and future research directions

In this article, we did not study how or in what priority various cybersecurity capabilities, such as prevention, detection, and response, should be developed. Working with a wide range of organizations, our observations show that many organizations that develop cybersecurity capabilities seem to take prevention and detection capabilities into consideration while ignoring response capabilities. A possible extension to our simulation game would be to study the consequences of such an approach in the long run.

On the importance of response capabilities, a cybersecurity expert, and the former White House chief information officer noted [97]:

> *"Preparing, planning, and especially testing for a cyber-incident is crucial for all companies, both large and small. Whether your company has been actively managing cyber security risk for years or you are just beginning to develop an incident response capability, it is critical for boards and executives to engage employees in developing a robust, integrated approach to incident response. Unfortunately, companies too commonly put this task off and then find themselves flat-footed during a breach."*

Future studies could enhance our model by fitting it to empirical data of historical cyber events. Our experiment could also benefit from larger sample sizes, or the inclusion of non-security business experts as another control group. A more sophisticated version of the game could be developed, allowing players to take on different roles and play in teams, or play against other players in an 'attackers versus defenders' scenario. Interesting complexities will likely arise in a game where there are several interdependent groups, such as how attractive a particular organization is for attackers relative to others in the simulation game.

Future studies should consider different experimental groups beyond the two presented in this study. It would be interesting to see how players who have been given different initial settings perform in the simulation game. For example, a player who begins the simulation with compromised systems may behave differently from a player who begins the simulation with all systems in the 'not-at-risk' set,

especially if they are informed about the situation. In another experiment, one group of players could be told to consider cybersecurity development costs as expenses, while another group is told that these same costs are investments. Further studies could also test the performance of players with various levels of targeted cybersecurity training. Experiments may also introduce different vectors of cyber-attacks and different types of defenses in which players could invest.

The purpose of this study was not to focus on *how* to improve the understanding of the complexities of cybersecurity capability development, but rather to draw attention to the lack of understanding of these complexities. Our findings highlight the importance of training of decision-makers about cybersecurity capability development, and future research should study the effects of different training interventions. We hope that our findings motivate the cybersecurity community to design and adopt enhanced educational and training programs that challenge entrenched mindsets, and encourage proactive cybersecurity capability development.

Acknowledgements

We would like to thank Zhen Fang and Xiaoxue Liu for their excellent assistance in this research. We also thank Edwin Farley, Jessica Kaiser, Priscilla Koepke, Natasha Nelson, Noel Zamot, and Chris Zannetos for their constructive feedback and comments on initial versions of this article. Financial support for this study was provided by MIT $(IC)^3$—the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

References

[1] M. Kan, Yahoo reports massive data breach involving 1 billion accounts, 2016.
[2] Verizon, Verizon 2015 Data Breach Investigations Report, Verizon, 2015.
[3] Target, Form 10-K, United States Security and Exchange Commision, 2017.
[4] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, International Journal of Electronic Commerce, 9 (2004) 70-104.
[5] R.K. Chellappa, P.A. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logistics Information Management, 15 (2002) 358-368.
[6] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, Future directions for behavioral information security research, Computers & Security, 32 (2013) 90-101.
[7] ServiceNow, The Global CISO Study: How Leading Organizations Respond to Security Threats and Keep Data Safe, Point of View, 2017.
[8] K.L. Hui, S.H. Kim, Q.H. Wang, CYBERCRIME DETERRENCE AND INTERNATIONAL LEGISLATION: EVIDENCE FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS, Mis Quarterly, 41 (2017) 497-+.
[9] S. Madnick, Preparing for the Cyberattack That Will Knock Out U.S. Power Grids, Harvard Business Review, 2017.
[10] T. Abdollah, Hackers broke into hospitals despite software flaw warnings, The Associated Press, 2016.
[11] Microsoft, Microsoft Security Bulletin MS17-010 - Critical, Microsoft, TechNet, 2017.

[12] S.L. Jarvenpaa, B. Ives, Executive Involvement and Participation in the Management of Information Technology, MIS Quarterly, 15 (1991) 205-227.
[13] W.J. Doll, Avenues for Top Management Involvement in Successful MIS Development, MIS Quarterly, 9 (1985) 17-35.
[14] A. Kankanhalli, H.-H. Teo, B.C.Y. Tan, K.-K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management, 23 (2003) 139-154.
[15] A.D. Veiga, J.H.P. Eloff, An Information Security Governance Framework, Information Systems Management, 24 (2007) 361-372.
[16] K.A. Barton, G. Tejay, M. Lane, S. Terrell, Information system security commitment: A study of external influences on senior management, Computers & Security, 59 (2016) 9-25.
[17] C. Hsu, J.-N. Lee, D.W. Straub, Institutional Influences on Information Systems Security Innovations, Information Systems Research, 23 (2012) 918-939.
[18] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly, 34 (2010) 523-548.
[19] J. Kwon, M.E. Johnson, Proactive Versus Reactive Security Investments in the Healthcare Sector, Mis Quarterly, 38 (2014) 451-471.
[20] A. Nagurney, S. Shukla, Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability, European Journal of Operational Research, 260 (2017) 588-600.
[21] C. Heitzenrater, A. Simpson, Software Security Investment: The Right Amount of a Good Thing, IEEE Cybersecurity Development, 2016, pp. 53-59.
[22] R. Bose, X. Luo, Investigating security investment impact on firm performance, International Journal of Accounting & Information Management, 22 (2014) 194-208.
[23] M.S. Jalali, A. Ashouri, O. Herrera-Restrepo, H. Zhang, Information diffusion through social networks: The case of an online petition, Expert Systems with Applications, 44 (2015) 187–197.
[24] A.A. Rad, M.S. Jalali, H. Rahmandad, How Exposure to Different Opinions Impacts the Life Cycle of Social Media, Annals of Operations Research, DOI (2017).
[25] S.G. Winter, The Satisficing Principle in Capability Learning, Strategic Management Journal, 21 (2000) 981-996.
[26] A.S. Bharadwaj, A RESOURCE-BASED PERSPECTIVE ON INFORMATION TECHNOLOGY CAPABILITY AND FIRM PERFORMANCE: AN EMPIRICAL INVESTIGATION, MIS Quarterly, 24 (2000) 169-196.
[27] C.E. Helfat, M.A. Peteraf, The dynamic resource-based view: capability lifecycles, Strategic Management Journal, 24 (2003) 997-1010.
[28] R.M. Grant, Contemporary strategy analysis : concepts, techniques, applications, 4th ed., Blackwell Business, Malden, Mass., 2002.
[29] J. Barney, Firm Resources and Sustained Competitive Advantage, J Manage, 17 (1991) 99-120.
[30] M.A. Peteraf, The Cornerstones of Competitive Advantage - a Resource-Based View, Strategic Management Journal, 14 (1993) 179-191.
[31] I. Dierickx, K. Cool, Asset Stock Accumulation and Sustainability of Competitive Advantage, Management Science, 35 (1989) 1504-1511.
[32] J.P. Eggers, S. Kaplan, Cognition and Renewal: Comparing CEO and Organizational Effects on Incumbent Adaptation to Technical Change, Organization Science, 20 (2009) 461-477.

[33] M. Zollo, S.G. Winter, Deliberate learning and the evolution of dynamic capabilities, Organization Science, 13 (2002) 339-351.
[34] H. Cavusoglu, H. Cavusoglu, J.Y. Son, I. Benbasat, Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources, Information & Management, 52 (2015) 385-400.
[35] G. Adomavicius, J.C. Bockstedt, A. Gupta, R.J. Kauffman, Making sense of technology trends in the information technology landscape: A design science approach, Mis Quarterly, DOI (2008) 779-809.
[36] H.A. Smith, J.D. McKeen, C. Cranston, M. Benson, Investment Spend Optimization: A New Approach to IT Investment at BMO Financial Group, 2010, pp. 65-81.
[37] Y. Lee, K.R. Larsen, Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software, European Journal of Information Systems, 18 (2009) 177-187.
[38] A.M. Johnson, Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study, Journal of Information Privacy & Security, 5 (2009) 3-27.
[39] E. Weishäupl, E. Yasasin, G. Schryen, IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review, DOI (2015).
[40] E. Weishäupl, E. Yasasin, G. Schryen, A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory, DOI (2015).
[41] B. Srinidhi, J. Yan, G.K. Tayi, Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors, Decision Support Systems, 75 (2015) 49-62.
[42] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi, Decision support approaches for cyber security investment, Decision Support Systems, 86 (2016) 13-23.
[43] K. Warren, Competitive strategy dynamics, Wiley, Chichester, 2002.
[44] B. Levitt, J.G. March, Organizational Learning, Annu. Rev. Sociol., 14 (1988) 319-340.
[45] D. Leonard-Barton, Core Capabilities and Core Rigidities - a Paradox in Managing New Product Development, Strategic Management Journal, 13 (1992) 111-125.
[46] H. Rahmandad, Effect of delays on complexity of organizational learning, Management Science, 54 (2008) 1297-1312.
[47] J.D. Sterman, Learning in and about complex systems, System Dynamics Review, 10 (1994) 91-330.
[48] G.S. Easton, S.L. Jarrell, The effects of total quality management on corporate performance: An empirical investigation, The Journal of Business, 71 (1998) 253.
[49] K.B. Hendricks, V.R. Singhal, The Long-Run Stock Price Performance of Firms with Effective TQM Programs, Management Science, 47 (2001) 359-368.
[50] N.P. Repenning, J.D. Sterman, Nobody ever gets credit for fixing problems that never happened: Creating and sustaining process improvement, California Management Review, 43 (2001) 64-+.
[51] J.K. Sterman, N.P. Repenning, F. Kofman, Unanticipated side effects of successful quality programs: Exploring a paradox of organizational improvement, Management Science, 43 (1997) 503-521.
[52] N.P. Repenning, Understanding fire fighting in new product development, The Journal of Product Innovation Management, 18 (2001) 285-300.
[53] N.P. Repenning, J.D. Sterman, Capability traps and self-confirming attribution errors in the dynamics of process improvement, Administrative Science Quarterly, 47 (2002) 265-295.

[54] J.G. March, Z. Shapira, Managerial Perspectives on Risk and Risk Taking, Management Science, 33 (1987) 1404-1418.
[55] S. Chai, M. Kim, H.R. Rao, Firms' information security investment decisions: Stock market evidence of investors' behavior, Decision Support Systems, 50 (2011) 651-661.
[56] C. McKinty, The C-Suite and IT Need to Get on the Same Page on Cybersecurity, Harvard Business Review, 2017.
[57] A. Corrin, Measuring what never happened, Public Sector Media Group, FCW: The Business of Federal Technology, 2013.
[58] S.A. Butler, Security attribute evaluation method: a cost-benefit approach, Proceedings of the 24th International Conference on Software Engineering. ICSE 2002, 2002, pp. 232-240.
[59] D. Komljenovic, M. Gaha, G. Abdul-Nour, C. Langheit, M. Bourgeois, Risks of extreme and rare events in Asset Management, Safety Science, 88 (2016) 129-145.
[60] D.W. Straub, R.J. Welke, Coping with systems risk: Security planning models for management decision making, Mis Quarterly, 22 (1998) 441-469.
[61] A. Tversky, D. Kahneman, Judgment under uncertainty: Heuristics and biases, Utility, probability, and human decision making, Springer1975, pp. 141-162.
[62] B.R. Rowe, and Michael P. Gallaher, Private sector cyber security investment strategies: An empirical analysis, The fifth workshop on the economics of information security (WEIS06), 2006.
[63] T. Moore, et. al, Identifying How Firms Manage Cybersecurity Investment, Southern Methodist University, Darwin Deason Institute for Cyber Security, 2015.
[64] R. Rue, Shari Lawrence Pfleeger, and David Ortiz, A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making, WEIS, DOI (2007).
[65] L.A. Gordon, and Martin P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security (TISSEC), 5 (2002) 438-457.
[66] S. Madnick, M.S. Jalali, M. Siegel, Y. Lee, D. Strong, R. Wang, W.H. Ang, V. Deng, D. Mistree, Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems, Lecture Notes in Artificial Intelligence 10097, Springer2017, pp. 67–77.
[67] J.D. Sterman, System Dynamics Modeling: Tools for Learning in a Complex World, California Management Review, 43 (2001).
[68] N.P. Repenning, A simulation-based approach to understanding the dynamics of innovation implementation, Organization Science, 13 (2002) 109-127.
[69] T. Abdel-Hamid, F. Ankel, M. Battle-Fisher, B. Gibson, G. Gonzalez-Parra, M. Jalali, K. Kaipainen, N. Kalupahana, O. Karanfil, A. Marathe, B. Martinson, K. McKelvey, S.N. Sarbadhikari, S. Pintauro, P. Poucheret, N. Pronk, Y. Qian, E. Sazonov, K. Van Oorschot, A. Venkitasubramanian, P. Murphy, Public and health professionals' misconceptions about the dynamics of body weight gain/loss, System Dynamics Review, 30 (2014) 58-74.
[70] A. Baghaei Lakeh, N. Ghaffarzadegan, Does analytical thinking improve understanding of accumulation?, System Dynamics Review, 31 (2015) 46-65.
[71] S. Villa, P. Gonçalves, S. Arango, Exploring retailers' ordering decisions under delays, System Dynamics Review, 31 (2015) 1-27.

[72] S. Arango Aramburo, J.A. Castañeda Acevedo, Y. Olaya Morales, Laboratory experiments in the system dynamics field, System Dynamics Review (Wiley), 28 (2012) 94-106.
[73] R.W. Proctor, J. Chen, The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace, Human Factors, 57 (2015) 721-727.
[74] Kaspersky, The Threats from Within: How educating your employees on cybersecurity can protect your company, DOI (2017).
[75] D. Disparte, C. Furlow, The Best Cybersecurity Investment You Can Make Is Better Training, Harvard Business Review, 2017.
[76] C. Posey, T.L. Roberts, P.B. Lowry, R.J. Bennett, J.F. Courtney, INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION ASSETS: DEVELOPMENT OF A SYSTEMATICS-BASED TAXONOMY AND THEORY OF DIVERSITY FOR PROTECTION-MOTIVATED BEHAVIORS, MIS Quarterly, 37 (2013) 1189-A1189.
[77] A.C. Johnston, M. Warkentin, M. Siponen, AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK: LEVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC, MIS Quarterly, 39 (2015) 113-A117.
[78] J.D. Sterman, B. Morrison, People express management flight simulator, Sloan School of Management, Cambridge, MA, 1988.
[79] J. Sterman, T. Fiddaman, T. Franck, A. Jones, S. McCauley, P. Rice, E. Sawin, L. Siegel, Climate interactive: the C‐ROADS climate policy model, System Dynamics Review, 28 (2012) 295-305.
[80] J.D. Sterman, Teaching Takes Off, OR/MS Today, 35 (1992) 40-44.
[81] L. McFarland, B. Milstein, G. Hirsch, J. Homer, D. Andersen, R. Irving, E. Reineke, R.D. Niles, E. Cawvey, A. Desai, The NASPAA Student Simulation Competition: Reforming the US Health Care System Within a Simulated Environment, Journal of Public Affairs Education, 22 (3) (2016) 363-380.
[82] N. Ghaffarzadegan, A. Ebrahimvandi, M.S. Jalali, A Dynamic Model of Post-Traumatic Stress Disorder for Military Personnel and Veterans, PLoS One, 11 (2016) e0161405.
[83] NIST, Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2014.
[84] H. Rahmandad, Impact of growth opportunities and competition on firm-level capability development trade-offs, Organization science, 23 (2012) 138-154.
[85] H. Rahmandad, D.M. Weiss, Dynamics of concurrent software development, System Dynamics Review, 25 (2009) 224-249.
[86] S.M. Bragg, Accounting reference desktop, John Wiley & Sons, New York, 2002.
[87] D. Bisson, Improving Cyber Security Literacy in Boards & Executives, 2015.
[88] A. Acquisti, J. Grossklags, Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior, 2nd Annual Workshop on Economics and Information Security-WEIS, 2003, pp. 1-27.
[89] S. Deutscher, et. al, Cybersecurity Meets IT Risk Management: A Corporate Immune and Defense System, BCG Perspectives, The Boston Consulting Group, 2014.
[90] M. Jalali, H. Rahmandad, H. Ghoddusi, Using the method of simulated moments for system identification, Analytical methods for dynamic modelers, DOI (2015).

[91] W. Jingguo, M. Gupta, H.R. Rao, INSIDER THREATS IN A FINANCIAL INSTITUTION: ANALYSIS OF ATTACK-PRONENESS OF INFORMATION SYSTEMS APPLICATIONS, MIS Quarterly, 39 (2015) 91-A97.
[92] R. Willison, M. Warkentin, BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE, MIS Quarterly, 37 (2013) 1-20.
[93] D.N. Sull, K.M. Eisenhardt, Simple rules : how to thrive in a complex world, Houghton Mifflin Harcourt, Boston, 2015.
[94] M.S. Jalali, How individuals weigh their previous estimates to make a new estimate in the presence or absence of social influence, International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction, Springer International Publishing, 2014, pp. 67-74.
[95] R.H. Thaler, C.R. Sunstein, Nudge : improving decisions about health, wealth, and happiness, Rev. and expanded ed., Penguin Books, New York, 2009.
[96] D. Kahneman, P. Slovic, A. Tversky, Judgment under uncertainty : heuristics and biases, Cambridge University Press, Cambridge ; New York, 1982.
[97] D. Bisson, Improving Cyber Security Literacy in Boards & Executives, 2015.