IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 23, 2017, accepted November 1, 2017, date of publication November 15, 2017, date of current version March 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2773366

An Options Approach to Cybersecurity Investment

MICHAIL CHRONOPOULOS[1,2], EMMANOUIL PANAOUSIS[3], (Member, IEEE), AND JENS GROSSKLAGS[4], (Senior Member, IEEE)

[1]School of Computing Engineering and Mathematics, University of Brighton, Brighton BN2 4GJ, U.K.
[2]Department of Business and Management Science, Norwegian School of Economics, 5045 Bergen, Norway
[3]Surrey Centre of Cyber Security, University of Surrey, Guildford GU2 7XH, U.K.
[4]Chair for Cyber Trust, Technical University of Munich, 80333 Munich, Germany

Corresponding author: Emmanouil Panaousis (e.panaousis@surrey.ac.uk)

ABSTRACT Cybersecurity has become a key factor that determines the success or failure of companies that rely on information systems. Therefore, investment in cybersecurity is an important financial and operational decision. Typical information technology investments aim to create value, whereas cybersecurity investments aim to minimize loss incurred by cyber attacks. Admittedly, cybersecurity investment has become an increasingly complex one, since information systems are typically subject to frequent attacks, whose arrival and impact fluctuate stochastically. Furthermore, cybersecurity measures and improvements, such as patches, become available at random points in time making investment decisions even more challenging. We propose and develop an analytical real options framework that incorporates major components relevant to cybersecurity practice, and analyze how optimal cybersecurity investment decisions perform for a private firm. The novelty of this paper is that it provides analytical solutions that lend themselves to intuitive interpretations regarding the effect of timing and cybersecurity risk on investment behavior using real options theory. Such aspects are frequently not implemented within economic models that support policy initiatives. However, if these are not properly understood, security controls will not be properly set resulting in a dynamic inefficiency reflected in cycles of over or under investment, and, in turn, increased cybersecurity risk following corrective policy actions. Results indicate that greater uncertainty over the cost of cybersecurity attacks raises the value of an embedded option to invest in cybersecurity. This increases the incentive to suspend operations temporarily in order to install a cybersecurity patch that will make the firm more resilient to cybersecurity breaches. Similarly, greater likelihood associated with the availability of a cybersecurity patch increases the value of the option to invest in cybersecurity. However, the absence of an embedded investment option increases the incentive to delay the permanent abandonment of the company's operation due to the irreversible nature of the decision.

INDEX TERMS Cybersecurity, investment analysis, real options.

I. INTRODUCTION

The financial crisis made Information Technology (IT) infrastructures around the world change their whole business plans and often reduce their expenses. Although these reductions may not have been reflected on the productivity line, this is not the case when it comes to cybersecurity. Cyber attackers have advanced their technology and have managed to be one step ahead of those who try to defend their infrastructures. From 2013 and on-wards, the frequency of identified Advanced Persistent Threats (APTs) has greatly increased. APT's number one target were always organizations with high value assets. This is the main reason behind the persistency of those attacks. Lately, WannaCry malware belonging to the ransomware family attacked in global scale affecting a lot of countries around the world, and, in a lot of cases, critical infrastructure such as United Kingdom's National Health System (NHS) [1]. Although in the beginning it seemed that malicious parties behind the attacks were trying only to make money, soon afterwards, it was implied that this was not the case, as the money made from the global scale attack were not so much. The NHS case needs special attention as not only it is a critical infrastructure, but also there are many cases of people who faced issues regarding their treatment with the commonest of all being large delays.

However, cybersecurity is not only a defensive maneuver but also a strategic decision that may increase the competitive advantage of a firm over potential rivals. The importance of cybersecurity has led many organizations to pay much

attention to cybersecurity investment decisions, especially to derive the appropriate level of these investments. This was firstly investigated by [2] and later on investigated by [3]–[5]. Cybersecurity spending is occurring in a variety of areas including software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, automated data backup, and hardware devices.

A critical observation, in [2], is that despite organizations being satisfied with their Return On Investment (ROI), cyber adversaries very often appear more incentivized to breach an organization's system towards satisfying a variety of objectives. While the ''defenders'' spend millions trying to protect their systems from cyber attackers, the latter may only have to spend a small amount of money to breach cybersecurity controls. This is for example due to social engineering attacks that can bypass cybersecurity best practices.

In addition to this, the range and scope of cyber attacks create the need for organizations to prioritize the manner in which they defend themselves. With this in mind, each organization needs to consider the threats that they are most at risk from and act in such a way so as to reduce the vulnerability across as many relevant weaknesses as possible. This is a particularly difficult task that many Chief Information Security Officers (CISOs) are not confident in achieving due to: (i) lack of sufficient budget; (ii) uncertainty regarding the cost of cyber attacks and the availability of cybersecurity controls; and (iii) irreversibility of expenditures related to cybersecurity controls. This work implements these features into an analytical real options framework and addresses the problem of when to invest in cybersecurity by deriving the optimal investment rule and analyzing the implications of deviating from it.

Even with all the focus on security, the number of unauthorized intrusions and cybersecurity breaches are steadily increasing. This has been attributed partly to poor understanding of the economics of investing in cybersecurity resulting in *ad-hoc* decisions. Additionally, these decisions are not viable from a cost-benefit perspective, since trying to patch most, if not all, of a firm's potential security vulnerabilities, to avoid cybersecurity breaches, could manifest a clear *over-investment* in cybersecurity.

Given the uncertainties surrounding cybersecurity breaches and efforts to prevent such breaches, a third explanation for the ubiquitous nature of cybersecurity vulnerabilities may be that it is economically rational to initially invest a portion of the cybersecurity budget and defer remaining investments until cybersecurity breaches actually occur. In other words, it may pay to take a wait-and-see attitude toward part of the investments made in cybersecurity activities, as firstly proposed in [6]. This explanation is akin to the notion of the deferment option discussed in the modern economics literature on capital budgeting [7]. To the extent that this explanation is correct, we would expect organizations to use cybersecurity breaches as a critical determinant of their actual (as opposed to budgeted) expenditures on cybersecurity. Since cybersecurity investments involve decision-making under uncertainty, it seems appropriate to borrow notions and techniques used by *real options theory*, a branch of financial investment theory which accounts for deferred investment to drive better cybersecurity investment decision-making.

In this paper, we consider a firm that holds a perpetual option to invest in a project that is subject to cyber attacks. The attacks take place in continuous time, and, once their cost reaches a critical threshold, the firm must either terminate operations or invest in cybersecurity, thereby making its infrastructure more resilient to cyber attacks. In summary, our proposal for designing optimal cybersecurity investment decisions showcases three contributions:

- **i.** Our analytical real options framework explores how cyber attacks impact the value of a project in the presence of an embedded option to invest in cybersecurity.
- **ii.** Our analytical results assess the impact of cost and technological uncertainty on the value of a project, the option to invest in cybersecurity, and the loss in value when such options are not taken into account.
- **iii.** Our framework provides managerial insights based on analytical and numerical results.

Figure 1 provides a concise, visual summary of the model and scope of the article. We have assumed that a cybersecurity provider releases a patch during the period of an active firm's project. The arrival of the patch is stochastic. The adversary captures all the different attacks that are launched against the firm's project and they also arrive in a stochastic manner. In parallel, we assume that the efficiency of the project is affected by cybersecurity incidents, caused by attacks. Our proposed method and tool, determines the right time to invest in cybersecurity (i.e. acquire a patch), which is, in fact, dictates when the company must cease and subsequently commence operations.

We proceed by discussing important related work in Section II and introduce assumptions and notation in Section III. In Section IV-A, we address the problem of optimal investment timing without taking into account a firm's flexibility to reinvest, and, in Section IV-B, we assume that the firm has a single embedded option to resume the project after a cybersecurity breach. Finally, Section V concludes the paper and offers directions for further research.

II. RELATED WORK

In [6], Gordon *et al.* first introduced the concept of timing into cybersecurity investment proposing a ''wait-and-see'' tactic. Their approach suggested not to over-invest into cybersecurity controls without knowing with certainty that these will be used at some point to mitigate an attack. And the only way to acquire this knowledge is to wait until a non-catastrophic incident happens; thereafter the defender shall react by investing into defenses. However, a limitation of this approach, as opposed to work here, is that it is based on a discrete-time framework that does not take into account the sequential nature of such catastrophic events and the need to repeat this strategy over time.

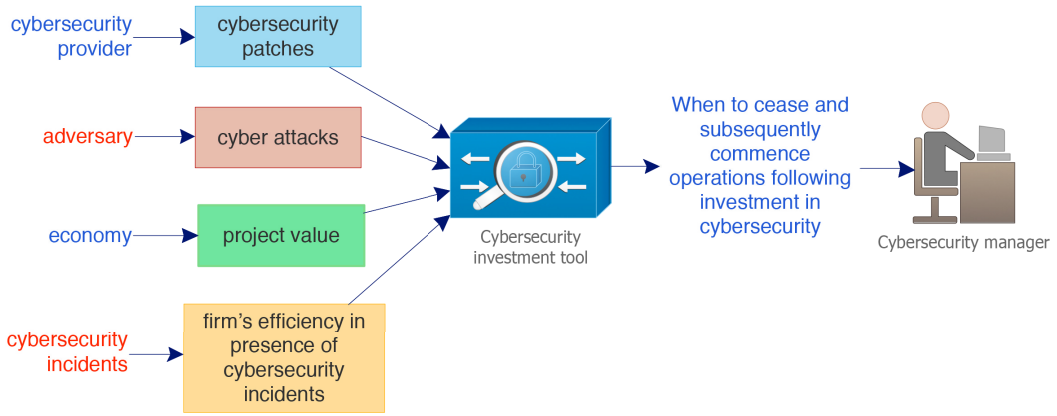

FIGURE 1. High level diagrammatic overview of our contribution to the field of security economics.

Early work in the area of sequential investments includes [8], which shows how traditional valuation methods understate the value of a project by ignoring the flexibility embedded in the time to build. An analytical framework for sequential investment is developed by Dixit and Pindyck [9], who assume that the output price follows a geometric Brownian motion (GBM), the project value depreciates exponentially, and the investor has an infinite set of replacement options. A comparison between a sequence of small nuclear power plants with a single, large power plant is down in [10], who show that the value of modularity may trigger investment in the initial module at a price level below the now–or–never net present value (NPV) threshold. Malchow-Møller *et al.* [11] illustrate how embedded investment options make the required investment threshold less sensitive to changes in uncertainty and the investment behaviour similar to the simple NPV rule. By comparing a single–stage investment to a stepwise investment strategy, Kort *et al.* [12] show that greater price uncertainty makes the former strategy more attractive relative to the latter by increasing the incentive to avoid costly switches between states.

Examples of analytical real options frameworks that allow for the random arrival of technological innovations include [13] indicating that the timing of technology adoption is influenced by expectations about future technological changes and that technological uncertainty tends to delay adoption. In [14] authors develop a model for sequential investment, whereby a firm may either adopt every technology that becomes available, skip an old technology in order to adopt the next one, purchase only an early innovation, or wait for a new technology to arrive before adopting the previous one. In each case, they illustrate how the rate of innovation and technological growth impact the optimal technology–adoption strategy and find that a firm may adopt an available technology despite the likely arrival of more efficient innovations. Nevertheless, how price and technological uncertainty interact to affect the optimal investment rule under each strategy is not thoroughly discussed.

In [15], Farzin *et al.* investigate the optimal timing of technology adoption assuming that new technologies arrive according to a Poisson process, however, they ignore output price uncertainty. In [16], Doraszelski revisits the analytical framework in [15] and shows that, compared to the NPV approach, a firm will defer the adoption of a new technology when it takes the option value of waiting into account. Huisman and Kort analyze, in [17], a duopoly in which firms face price and technological uncertainty and show that the efficiency of a new technology can offset the monopoly profits that a leader receives while being alone in the market, thereby turning a preemption game into one where the second mover receives a higher pay-off. In [18], Kauffman and Li use a standard Brownian motion in order to describe uncertainty in the outcome of technology competition and analyze the investment strategy of a firm that can choose between two competing technologies. Miltersen and Schwartz adopt a real options approach for valuing R&D projects under uncertain time to completion, operational flexibility, and competition [19].

Gordon *et al.* [20] extend their previous work [6] on the application of real options to cybersecurity investment by taking into account information sharing, for example regarding vulnerabilities. They show that information sharing can decrease uncertainty about risks, thereby decreasing the value of deferment options; therefore optimal investments may take place early. They also use an example to show how to calculate the minimum value of information sharing required so that the company invests straightaway in cybersecurity. The authors discuss the limitations of their work. Importantly, they assume that the reduction of risks occurs only due to increased information sharing; ignoring completely that waiting may have more benefits, such as more efficient cybersecurity controls are available to purchase. Another limitation of [20] and [6] is that they do not develop a formal model, and, as a result, they do not derive an optimal solution. While our work does not consider information sharing, it accounts for managerial discretion in terms of the option to adopt a cybersecurity control and

the option to postpone termination or commencement of operations.

In [21], Daneva summarises the main ways of applying real options analysis to cybersecurity investments. The paper provides examples of the most common types of real options as applied to the cross-organizational information security context for specific purposes such as achieving better timing for an investment. The author proposes a five-phases methodology to approach real-options-based security decision support. For each phase, she presents relevant research questions and discusses the challenges in developing a particular approach. Our paper reflects an adaptation of this methodology, whereby we: (i) take into account the likely arrival of security options; (ii) identify key underlying uncertainties; (iii) select a suitable mathematical model, namely dynamic programming; (iv) derive the optimal decision rule; and (v) provide intuitive managerial insights.

In [22], Herath and Herath develop an empirical real options model based on Bayesian statistics to derive optimal cybersecurity investments considering a specific cybersecurity mechanism, i.e., an intrusion detection system (IDS). They extend [23] and [24] by including cost and benefits of configuring an IDS, investigating what is the best timing to invest, and finally revising the IDS parameters based on Bayesian learning. The authors suggest that it is preferable to undertake cybersecurity investments in stages so that they assess the performance of an IDS, and should new threats, vulnerabilities be identified or a cybersecurity breach occurs, then they can decide to invest in improving it. The authors used the American-style sequential real options. Our work uses perpetual American style options. Their work suggests to invest into a series of interrelated investment projects that are made after resolving uncertainty. A significant contribution of this paper is that the authors use actual data on e-mail and spam to validate their framework and the optimality of the determined investment measured in terms of IDS efficiency.

Given two security technologies S_1 and S_2, the authors in [25] propose a decision model that aims to aid managers in deciding whether (a) to invest in a non-flexible security process innovation (SPI) that uses either technology S_1 or S_2, or (b) to invest in a flexible SPI that allows switching between the two compatible technologies. The model also aims to explore when it would be cost-effective to continue using the current technology and when the firm is better off switching to a compatible technology. The authors use dynamic programming to derive the value of investing in an SPI.

Benaroch [26] used a real options model to reframe the cybersecurity investment problem as one of selecting a subset of uncertainty-reducing mitigations that may have substitutive, complementary or synergetic relationships. The availability of these mitigations is controlled by decision-makers, but their size is log-normally distributed. The innovation of his work is to improve the efficiency of cybersecurity investments by balancing mitigations' costs against their incremental (diminishing) uncertainty-reduction impacts on cybersecurity loss expectancy. From a practical point of view, the author's model facilitates lowering cybersecurity costs without compromising on loss-prevention potential. However, one limitation is that the availability of mitigations is typically subject to technological innovations that take place at random points in time. Ignoring this stochasticity may result in a dynamic inefficiency with possible cycles of under- or over-investment, and, in turn, increased regulatory risk when corrective policy actions are required. In our model, we relax the assumptions underlying the availability of cybersecurity controls and introduce uncertainty over their arrival.

Finally, Berthold and Böhme [27] have motivated why, and explained how, option pricing theory can be useful for the valuation of informational privacy. They have proposed a very simple model that highlights the description of changes in each individual data subject's attribute values and the evolution of the distribution of attribute values in the population as two independent stochastic processes. The authors suggest possible applications of the proposed valuation methods to guide decision support in future privacy-enhancing technologies.

III. PROBLEM FORMULATION

We consider a firm with a perpetual option to invest in cybersecurity facing uncertainty over the cost of a successful security breach and over the release (i.e., arrival) of new cybersecurity controls (e.g., anti-malware) that may be adopted to enhance the cybersecurity of the firm. Given a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, we assume that the arrival of new cybersecurity controls follows a Poisson process, $\{M_t,\ t \geq 0\}$, where t is continuous and denotes time and $\lambda \geq 0$ denotes the intensity of the Poisson process. The latter represents the rate of arrival of cybersecurity controls, and, therefore, M_t counts the number of random times that a control arrives between 0 and t. Hence, if no control has been developed until time t, then, with probability λdt, it will arrive within the next short interval of time dt, i.e.:

$$dM_t = \begin{cases} 1, & \text{with probability } \lambda dt \\ 0, & \text{with probability } 1 - \lambda dt \end{cases}$$

In Table I, we summarise the notations introduced throughout the article. In this paper, we refer to the firm's operation as *the project*, which is a typical expression used in the literature of real options (Dixit & Pindyck, 1994). Let us assume that the project generates a fixed revenue per unit of time denoted by P and the immediate loss following a cybersecurity breach follows a continuous-time stochastic process and is denoted by $\{C_t, t \geq 0\}$. In line, with the discrete-time model of Gordon *et al.* [6], we assume that C_t follows a geometric Brownian motion (GBM), which is described in (1), where μ is the *annual growth rate*, σ is the *annual volatility*, and dZ_t is the increment of the standard Brownian motion. Although we could use another stochastic process to describe the dynamics of the loss following a cybersecurity breach, we persist with the GBM for its analytical tractability and continuity with the real options literature.

$$dC_t = \mu C_t dt + \sigma C_t dZ_t, \quad C_0 \equiv C > 0 \tag{1}$$

TABLE 1. List of symbols.

Symbol	Description
t	time
M_t	arrival process of security software
C_t	immediate loss due to a cybersecurity breach
λ	intensity of M_t
P	output price
μ	annual growth
σ	annual volatility
dZ_t	increment of Brownian motion
r	discount rate
$F_{1,0}^{(0)}(C)$	option to abandon a project
I_0	fixed cost for exercising $F_{1,0}^{(0)}(C)$
$\tau_{1,0}^{(0)}$	time of abandonment
$C_{1,0}^{(0)^*}$	abandonment threshold
$\Phi_0^{(0)}(C)$	project expected value in the inactive state
D	project efficiency in benchmark case
$\overline{D}$	project efficiency prior to a security breach
$\underline{D}$	project efficiency after a security breach

Also, we let $r \geq \mu$ denote the subjective discount rate, which is defined exogenously. We assume that $\{C_t, t \geq 0\}$ is independent of $\{M_t, t \geq 0\}$. This enables the analysis when the firm has no information about the arrival of new cybersecurity controls, and, therefore, the firm does not take into account how new controls will affect the immediate loss incurred by an attack.

We assume that the firm is initially in an active state, denoted by 1, and holds the option to abandon the project in the case of a cybersecurity breach, thereby entering an inactive state, denoted by 0.

In state 1, the firm holds some information that may affect future cybersecurity investments. These include:

- the current *cybersecurity level* (i.e., the overall efficacy of the firm in terms of protecting itself against cyber attacks), which is determined by the types of cybersecurity controls the company has in place;
- the current threat landscape (i.e., attack trends) that determines the probability of an attack being launched and being successful. Altogether, the above express what we refer to in the cybersecurity literature [3] as *expected risk*.

Apparently, if there is no available budget to invest in cybersecurity, there is no embedded option available. Thus, in the absence of an embedded option to enhance its cybersecurity level, the firm's *option to abandon* the project is denoted by $F_{1,0}^{(0)}(C)$. The firm can exercise this option by incurring a *fixed cost*, I_0. The motivation of abandonment is that the firm does not wish to maintain an active project that does not generate any profit, and, even worse, introduces

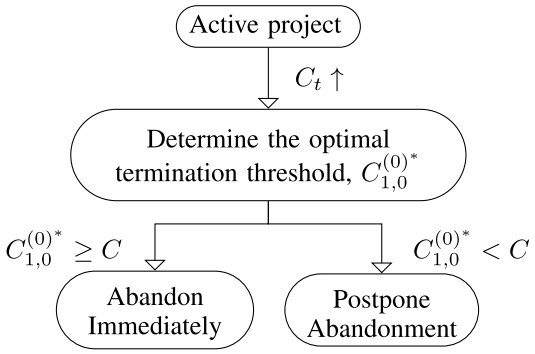

FIGURE 2. Benchmark case.

only damages. As indicated in Figure 2, the firm will either abandon the project immediately if the optimal abandonment threshold, denoted by $C_{1,0}^{(0)^*}$, is greater than the current loss C or postpone abandonment otherwise.

Once the firm abandons the project at time $\tau_{1,0}^{(0)}$, it recovers the salvageable operating cost but eliminates the revenues that the project generates. The expected value of the project in the inactive state is denoted by $\Phi_0^{(0)}(C)$. We capture the described abandonment in a state transition diagram in Figure 3.

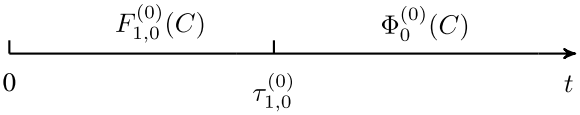

FIGURE 3. State transition diagram: Permanent abandonment.

However, the firm may have the option to invest in a cybersecurity control and reduce the likelihood of terminating the project due to a cybersecurity breach, as shown in Figure 4. Hence, we assume that the project is operating initially at a low efficiency level $\underline{D}$ and a cybersecurity control will increase the efficiency of the project to $\overline{D}$. Note that this level is not the same as the cybersecurity level and it refers to the productivity of the company regardless of cybersecurity attacks. Exercising this option entails a cost I_1. The time at which the option is exercised is denoted by $\tau_{1,0}^{(1)}$ and the corresponding optimal investment threshold is denoted by $C_{1,0}^{(1)^*}$.

IV. MODEL

A. BENCHMARK CASE: NO CYBERSECURITY CONTROL

We assume that the firm has no option to invest in any type of cybersecurity control that will improve the efficiency of the project. Initially, the firm is in state $(1, 0)$, where it receives the cash-flows of the active project and holds a single option to abandon it, when the cost of cyber attacks reaches the threshold $C_{1,0}^{(0)}$. Once the option is exercised at time $\tau_{1,0}^{(0)}$, the firm moves to state 0 and terminates the operations of the project (see Figure 5).

We derive the value function of the firm at each state by using backward induction. Therefore, we assume that the cost associated with cybersecurity breaches is low, and, therefore,

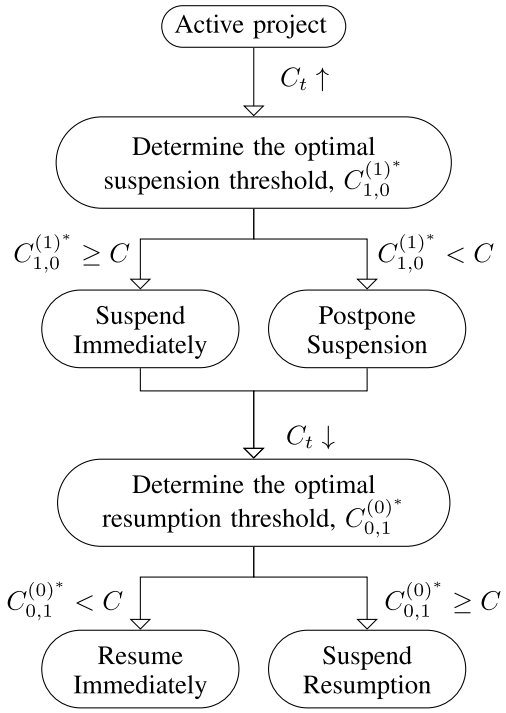

FIGURE 4. Investment with a single cybersecurity control.

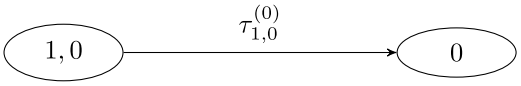

FIGURE 5. State transition diagram.

the firm can continue operating the project. All the cash flows of the project are indicated in Figure 6.

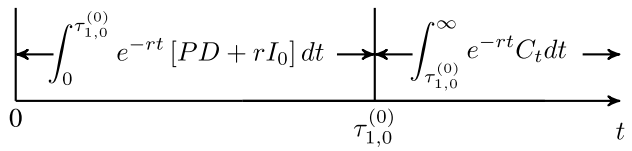

FIGURE 6. Irreversible abandonment under uncertainty.

The firm's objective is to maximize the time-zero discounted expected value of all the cash flows of the project, which is indicated in (2). More specifically, the firm wants to determine the time at which it is optimal to terminate the revenues of the project (first term) in order to recover the salvageable increasing cost of the cyber attacks (second term). Note that $\mathbb{E}_C[\cdot]$ is the expectation operator that is conditional on the initial cost value.

$$\mathbb{E}_C\left[\int_0^{\tau_{1,0}^{(0)}} e^{-rt}\,[PD + rI_0]\,dt + \int_{\tau_{1,0}^{(0)}}^{\infty} e^{-rt} C_t dt\right] \tag{2}$$

By decomposing the first term in (2), we obtain (3).

$$\int_0^{\infty} e^{-rt}\,[PD + rI_0]\,dt + \mathbb{E}_C\left[\int_{\tau_{1,0}^{(0)}}^{\infty} e^{-rt}\,[C_t - PD - rI_0]\,dt\right] \tag{3}$$

Notice that the first term in (3) is deterministic, and, therefore, the optimisation objective is reflected in the second term and is described in (4), where $\mathcal{S}$ is the set of stopping times generated by the filtration of the C_t.

$$F_{1,0}^{(0)}(C) = \sup_{\tau_{1,0}^{(0)} \in \mathcal{S}} \mathbb{E}_C \int_{\tau_{1,0}^{(0)}}^{\infty} e^{-rt}\,[C_t - PD - rI_0]\,dt \tag{4}$$

Next, we rewrite (4) as in (5) using the law of iterated expectations and the strong Markov property of the GBM. The latter states that the value of the process C_t after time t depends on the value of the process at time t and is independent of the value of the process before time t.

$$F_{1,0}^{(0)}(C) = \sup_{\tau_{1,0}^{(0)} \in \mathcal{S}} \mathbb{E}_C\left[e^{-r\tau_{1,0}^{(0)}}\right] \Phi_0^{(0)}\left(C_{1,0}^{(0)}\right) \tag{5}$$

Note that $\Phi_0^{(0)}(C)$ is the value of the project at abandonment. The expression of the value of the terminated project is indicated in (6). The first term on the right-hand side of (6) is the expected present value of the salvageable operating cost and the second term is the present value of the foregone cash flows.

$$\begin{aligned}\Phi_0^{(0)}(C) &= \mathbb{E}_C \int_0^{\infty} e^{-rt}\,[C_t - PD - rI_0]\,dt \\ &= \frac{C}{r-\mu} - \frac{PD}{r} - I_0\end{aligned} \tag{6}$$

Also, $\mathbb{E}_C\left[e^{-r\tau_{1,0}^{(0)}}\right] = \left(\frac{C}{C_{1,0}^{(0)}}\right)^{\beta_1}$ is the stochastic discount factor, and, therefore, the optimisation objective can finally be expressed as in (7).

$$F_{1,0}^{(0)}(C) = \max_{C_{1,0}^{(0)^*} > C} \left(\frac{C}{C_{1,0}^{(0)}}\right)^{\beta_1} \Phi_0^{(0)}\left(C_{1,0}^{(0)}\right) \tag{7}$$

Also $\beta_1 > 1, \beta_2 < 0$ are the roots of the quadratic $\frac{1}{2}\sigma^2\beta(\beta-1) + \mu\beta - r = 0$ (Dixit & Pindyck, 1994), i.e:

$$\beta_1 = \frac{1}{2} - \frac{\mu}{\sigma^2} + \sqrt{\left(\frac{1}{2} - \frac{\mu}{\sigma^2}\right)^2 + \frac{2r}{\sigma^2}} \tag{8}$$

$$\beta_2 = \frac{1}{2} - \frac{\mu}{\sigma^2} - \sqrt{\left(\frac{1}{2} - \frac{\mu}{\sigma^2}\right)^2 + \frac{2r}{\sigma^2}} \tag{9}$$

Applying first-order necessary conditions (FONC) to (7), we obtain the analytical expression of the optimal investment threshold, $C_{1,0}^{(0)^*}$, which is indicated in (10). Notice that, since $\beta_1 > 1$, the first term on the right-hand side of (10), $\frac{\beta_1}{\beta_1 - 1}$, is also greater than 1. This implies that $C_{1,0}^{(0)^*} > (r-\mu)\left[\frac{PD}{r} + I_0\right]$. Additionally, the term $(r-\mu)\left[\frac{PD}{r} + I_0\right]$ represents the Marshallian threshold, i.e., the investment criterion under the NPV rule. This reflects the traditional result of real options theory that uncertainty increases the incentive to postpone an irreversible decision. In this case, the firm would not want to terminate the project due to a temporary increase in the cost of a cybersecurity breach, which is more likely to happen when uncertainty is high.

$$C_{1,0}^{(0)^*} = \frac{\beta_1}{\beta_1 - 1}(r-\mu)\left[\frac{PD}{r} + I_0\right] \tag{10}$$

The optimal investment rule can also be expressed as in (11), where we equate the marginal benefit (MB) of delaying abandonment to the marginal cost (MC). The first term on the left-hand side of (11) is the MB created by waiting until the salvageable cost is higher, while the second term represents the reduction in the MC of waiting due to saved abandonment cost. Similarly, the first term on the right–hand side reflects the opportunity cost of forgone cash flows discounted appropriately.

$$\left(\frac{C}{C_{1,0}^{(0)*}}\right)^{\beta_1}\left[\frac{1}{r-\mu}+\frac{\beta_1}{C_{1,0}^{(0)*}}\left(\frac{PD}{r}+I_0\right)\right]=\left(\frac{C}{C_{1,0}^{(0)*}}\right)^{\beta_1}\frac{\beta_1}{r-\mu} \tag{11}$$

B. SINGLE CYBERSECURITY CONTROL

Here, we extend the framework of Section IV-A by allowing for a single embedded option to invest in a cybersecurity control, that will increase the efficiency of the project. The value of the active project is indicated in (12). The first term on the right-hand side is the expected present value of the revenues, while the second term is the present value of the operating cost.

$$\Phi_1^{(0)}(C)=\frac{P\overline{D}}{r}-\frac{C}{r-\mu}-I_1 \tag{12}$$

Assuming that the cost is initially high, the firm must wait until it drops below the revenues in order to resume operations. The firm's value function is described in (13)

$$F_{0,1}^{(0)}(C)=\begin{cases}A_{0,1}^{(0)}C^{\beta_2}, & C>C_{0,1}^{(0)}\\ \Phi_1^{(0)}(C), & C\le C_{0,1}^{(0)}\end{cases} \tag{13}$$

where $A_{0,1}^{(0)}$ and $C_{0,1}^{(0)}$ are determined via value-matching and smooth-pasting conditions and are indicated in (14) and (15), respectively. All proofs can be found in the Appendix.

$$C_{0,1}^{(0)*}=\frac{\beta_2}{1-\beta_2}(r-\mu)\left[I_1-\frac{P\overline{D}}{r}\right] \tag{14}$$

$$A_{0,1}^{(0)}=C_{0,1}^{(0)*-\beta_2}\Phi_1^{(0)}\left(C_{0,1}^{(0)*}\right) \tag{15}$$

Next, we step back and assume that the project is in a suspended state and that the firm holds a single embedded investment option. The dynamics of the value of the suspended project are described in (16). Notice that within an infinitesimal time interval dt a cybersecurity control may become available with probability λdt and the firm will receive the option, $F_{0,1}^{(0)}(C)$, to adopt it and upgrade the efficiency of the project to $\overline{D}$. By contrast, with probability $1-\lambda dt$ no cybersecurity control will become available and the firm will continue to hold the value function $\Phi_0^{(1)}(P)$.

$$\Phi_0^{(1)}(C)=(1-rdt)\mathbb{E}_C\Big[\lambda dtF_{0,1}^{(0)}(C+dC)+(1-\lambda dt)\Phi_0^{(1)}(C+dC)\Big] \tag{16}$$

By expanding the right-hand side of (16) using Itô's lemma, we can rewrite it as in (17), where $\mathcal{L}=\frac{1}{2}\sigma^2C^2\frac{\mathbf{d}^2}{\mathbf{d}C^2}+\mu C\frac{\mathbf{d}}{\mathbf{d}C}$ denotes the differential generator.

$$\left[\mathcal{L}-(r+\lambda)\right]\Phi_0^{(1)}(C)+\lambda F_{0,1}^{(0)}(C)=0 \tag{17}$$

By solving (17), we obtain the expression for $\Phi_0^{(1)}(C)$ that is described in (18), where $B_0^{(1)}$ and $E_0^{(1)}$ are obtained via value-matching and smooth-pasting conditions between the two branches and are indicated in (A-7) and (A-8). The first term in the top part of (18) reflects the value of the firm's option to enhance the cybersecurity of its information systems. However, this option is not available yet, and, therefore, the first term is adjusted via the second one. The first three terms in the bottom part of (18) represent the expected revenues upon investment, while the last term is the likelihood of the cost increasing above the waiting region.

$$\Phi_0^{(1)}(C)=\begin{cases}A_{0,1}^{(0)}C^{\beta_2}+B_0^{(1)}C^{\delta_2}, & C>C_{0,1}^{(0)}\\ \dfrac{\lambda P\overline{D}}{r(r+\lambda)}-\dfrac{\lambda C}{(r-\mu)(r+\lambda-\mu)}-\dfrac{\lambda I_1}{r+\lambda}\\ \quad +E_0^{(1)}C^{\delta_1}, & C\le C_{0,1}^{(0)}\end{cases} \tag{18}$$

Notice that it is possible to recover the deterministic scenario, reflected in (13), by setting either $\lambda=0$ or $\lambda\to\infty$. Indeed, $\lambda=0$ implies that a new cybersecurity patch (note that we use the terms cybersecurity patch and cybersecurity control interchangeably) will never become available, and, thus, both the top and the bottom part of (18) vanish, since $\lambda=0\Rightarrow\delta_2=\beta_2\Rightarrow B_0^{(1)}=-A_{0,1}^{(0)}$. Similarly, as λ increases, the arrival of a new cybersecurity patch becomes more likely. Indeed, notice that $\lambda\to\infty\Rightarrow B_0^{(1)}\to 0$.

Next, we consider the option to suspend operations temporarily with a singe embedded option to invest in a cybersecurity control. This is expressed in (19) and the optimal investment threshold is now obtained numerically.

$$F_{1,0}^{(1)}(C)=\max_{C_{1,0}^{(1)}>C}\left(\frac{C}{C_{1,0}^{(1)}}\right)^{\beta_1}\left[\frac{C_{1,0}^{(1)}}{r-\mu}-\frac{P\underline{D}}{r}-I_0+\Phi_0^{(1)}\left(C_{1,0}^{(1)}\right)\right],\quad C<C_{1,0}^{(1)} \tag{19}$$

The optimal suspension rule is indicated in (20), where we equate the MB of delaying suspension to the MC. Notice that this is the same as (11) apart from the extra two terms on the right-hand side, that reflect the extra cost associated with uncertainty over the arrival of a cybersecurity patch.

$$\left(\frac{C}{C_{1,0}^{(1)*}}\right)^{\beta_1}\left[\frac{1}{r-\mu}+\frac{\beta_1}{C_{1,0}^{(1)*}}\left(\frac{P\underline{D}}{r}+I_1\right)\right]=\left(\frac{C}{C_{1,0}^{(1)*}}\right)^{\beta_1}\left[\frac{\beta_1}{r-\mu}-(\delta_2-\beta_1)B_0^{(1)}C_{1,0}^{(1)*\delta_2-1}-(\beta_2-\beta_1)A_0^{(1)}C_{1,0}^{(1)*\beta_2-1}\right] \tag{20}$$

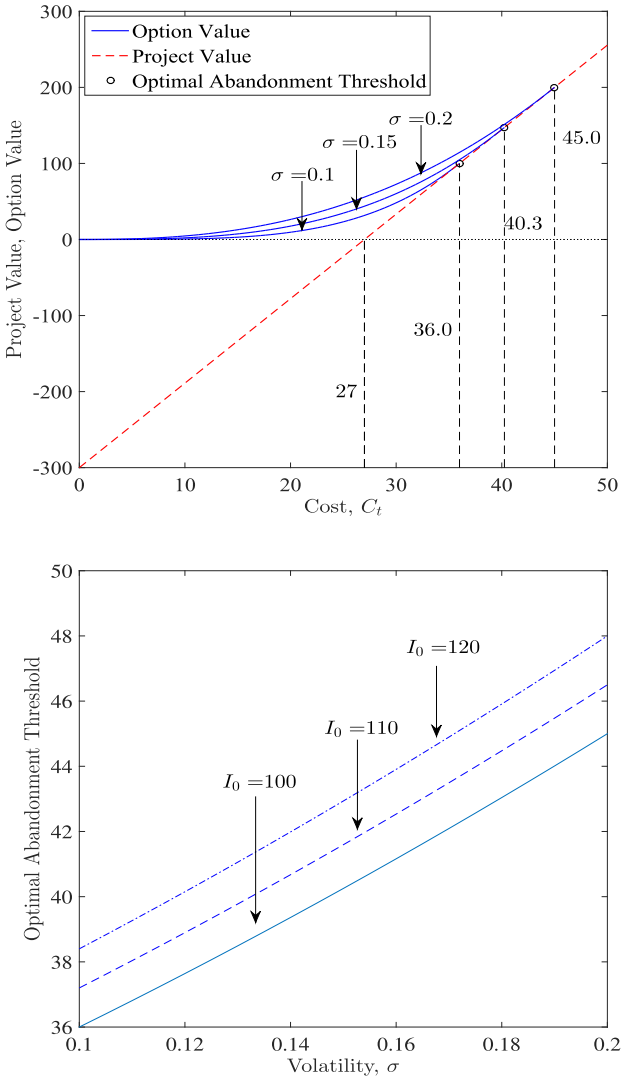

FIGURE 7. Option and project value for $\sigma = 0.1, 0.15$ and 0.2 (top panel) and optimal abandonment threshold versus σ (bottom panel).

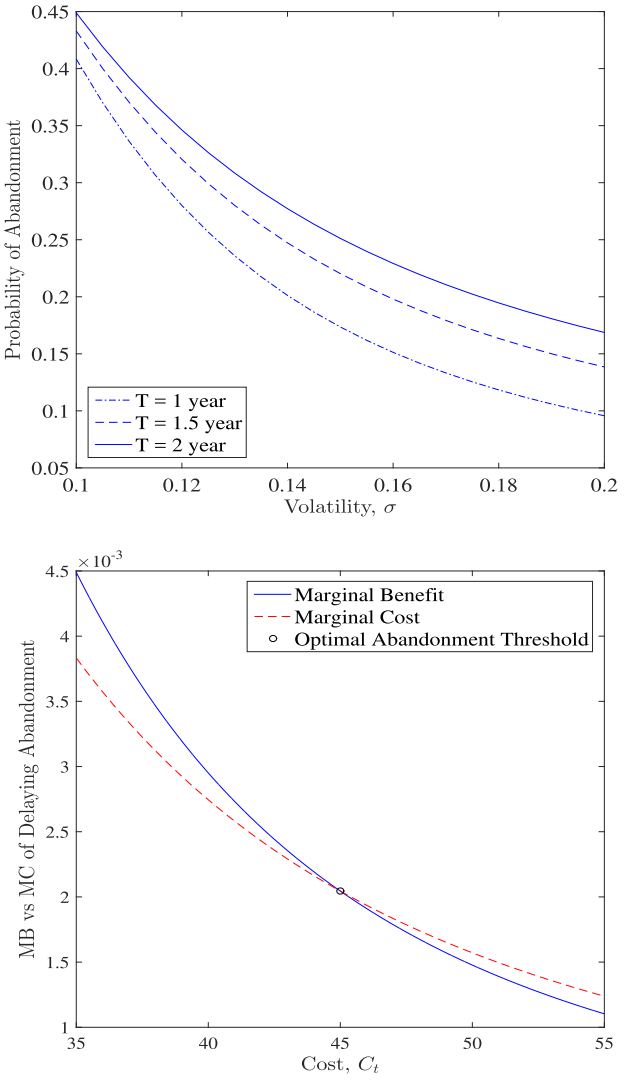

FIGURE 8. Probability of abandonment versus σ (top panel) and marginal benefit versus marginal cost of delaying abandonment for $\sigma = 0.2$ (bottom panel).

According to Proposition 1, abandonment is accelerated when the option to invest in a cybersecurity control is available. This happens because the option to invest in cybersecurity increases the overall value of the project and lowers the required abandonment threshold. Intuitively, unlike the benchmark case, the firm does not have to keep the project alive despite potential losses, if it has the option to resume operations with a more resilient system following a temporary suspension that is required to enhance cybersecurity.

Proposition 1: An embedded option to invest in a cybersecurity control accelerates abandonment, i.e., $C_{1,0}^{(1)^*} < C_{1,0}^{(0)^*}$.

Now, as the following Proposition 2 indicates, the relative gain in option value increases with greater λ. Notice that if $\lambda = 0$, then a new cybersecurity patch will not become available and the efficiency of the project will always be $\underline{D}$. By contrast, a greater λ raises the relative gain in option value, since a cybersecurity patch is more likely.

Proposition 2: Uncertainty over the cost of a cybersecurity breach and the arrival of a cybersecurity patch raises the relative gain in option value, $\frac{F_{1,0}^{(1)}(C) - F_{1,0}^{(0)}(C)}{F_{1,0}^{(1)}(C)}$.

In line with Proposition 1, we can show that the probability of abandonment increases when the firm holds an embedded option to enhance the cybersecurity of its information systems. For a GBM, the probability of suspension $\mathbb{P}_C\left[C \geq C_{1,0}^{(1)^*}\right]$ within T years given that the current cost is C is provided in closed form and is indicated in (21). Note that $\mathcal{N}(\cdot)$ is the cumulative distribution function (cdf) of the standard normal distribution.

$$\mathbb{P}_C\left[C \geq C_{1,0}^{(1)^*}\right] = \mathcal{N}\left(\frac{\left(\mu - \frac{1}{2}\sigma^2\right)T - \ln\left(\frac{C_{1,0}^{(1)^*}}{C}\right)}{\sigma\sqrt{T}}\right) \tag{21}$$

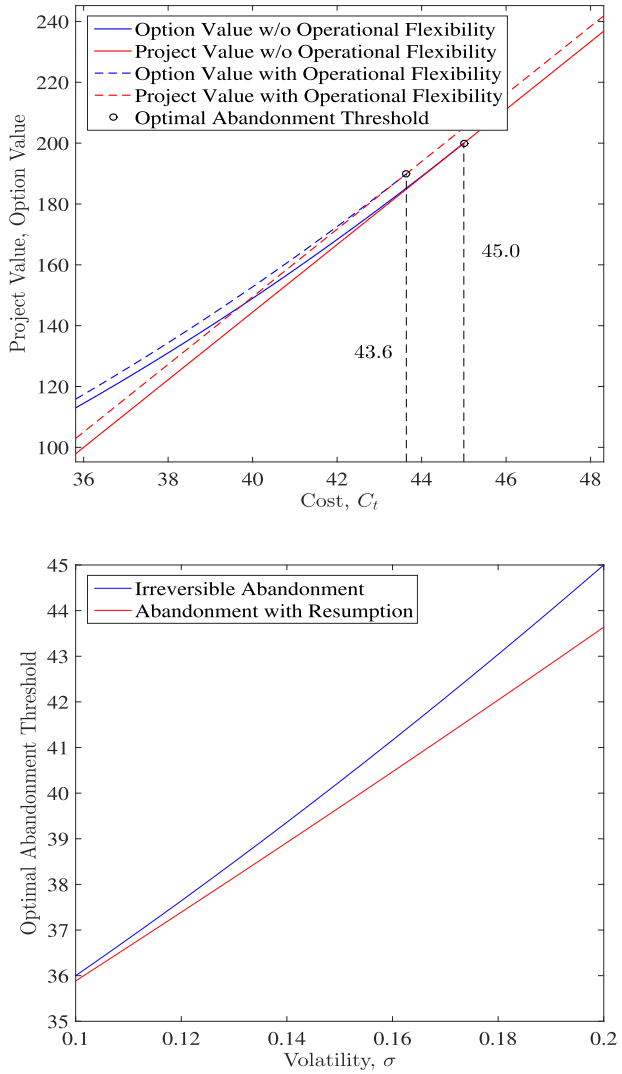

FIGURE 9. Option and project value with and without cybersecurity control for $\sigma = 0.2$ and $\lambda = 0.3$ (top panel) and optimal abandonment threshold versus σ (bottom panel).

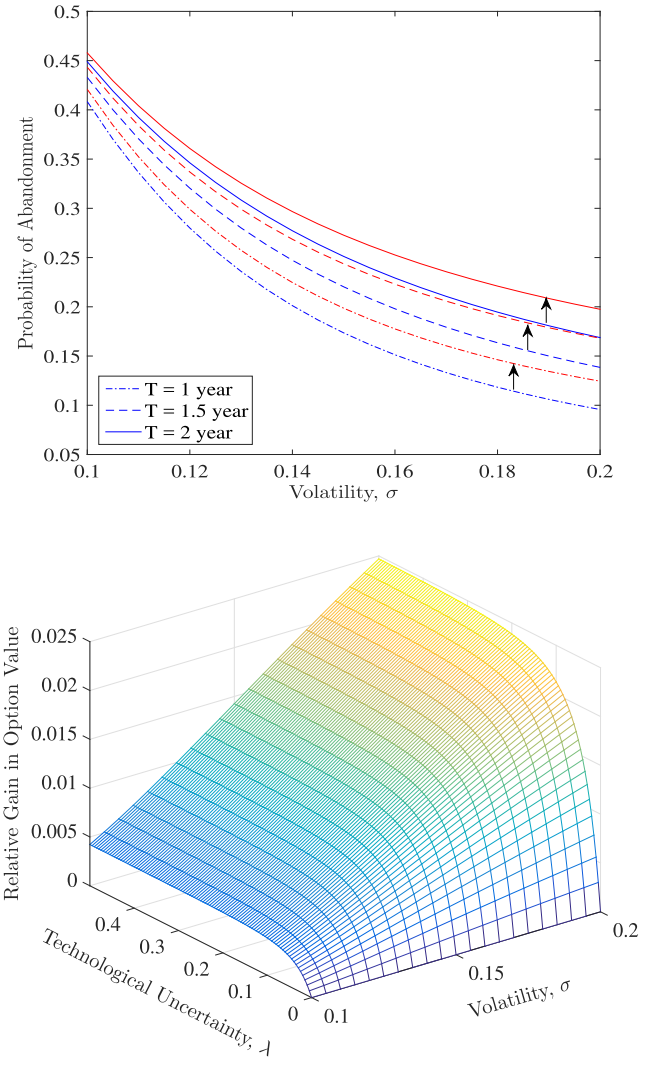

FIGURE 10. Optimal abandonment threshold with and without cybersecurity control versus σ for $\lambda = 0.3$ (top panel) and gain in option value due to technological uncertainty versus σ and λ (bottom panel).

C. NUMERICAL EXAMPLES

For a simple numerical illustration, we assume the following parameter values: $\mu = 0.01$, $r = 0.1$, $\sigma \in [0.1, 0.2]$. Also, $I_1 = 100$, $I_2 = 200$, $\underline{D} = 1$, $\overline{D} = 2$ and $\lambda \in [0, 1]$. Although it would be interesting to calibrate these to real data, here, we are primarily concerned with illustrating analytical insights via hypothetical parameters. The top panel in Figure 7 illustrates the value of the option to terminate operations and the value of the suspended project for $\sigma = 0.1, 0.15$ and 0.2. Notice that, in the absence of uncertainty, the firm should abandon the project at $C = 27$. This is the Marshallian threshold and reflects the NPV rule. The latter states that the firm should terminate operations when the NPV of the project is zero. However, increasing uncertainty raises the opportunity cost of abandonment and raises the required abandonment threshold. Intuitively, the firm would not want to terminate operations permanently in the case of a temporary increase in cost, which is more likely when uncertainty is high. The same result is illustrated in the bottom panel, which shows the impact of σ on the required abandonment threshold.

In the top panel of Figure 8, we assume that the current cost value is $C = 35$ and illustrate the impact of σ on the probability of abandonment within $T = 1, 1.5$ and 2 years. Notice that abandonment becomes less likely with greater cost uncertainty and more likely as the time horizon increases. According to the bottom panel, the MB and MC of delaying abandonment both decrease as the cybersecurity cost increases. However, for low values of C_t, the MB is greater than the MC, which implies that the marginal value of delaying investment is positive, thereby creating an incentive to postpone the termination of the project.

Figure 9, illustrates the option and project value with and without the embedded investment option (top panel) and the impact of cost uncertainty on the optimal abandonment threshold (bottom panel). As the top panel illustrates, the embedded investment option raises the value of the project and lowers the required abandonment threshold. The same

result is observable in the bottom panel, which illustrates the impact of cost uncertainty on both the optimal abandonment and suspension threshold.

The top panel in Figure 10 illustrates the impact of the embedded option to invest and improve the efficiency of the project on the probability of abandonment. Notice that the direction of the arrows indicates the increase in operational flexibility and the associated increase in the probability of suspension. The bottom panel illustrates the combined impact of uncertainty over the availability of a cybersecurity patch and the cost of cyberattacks on the relative gain in option value. Note that greater uncertainty raises the value of the embedded option to invest in cybersecurity. Interestingly, a greater likelihood of the availability of a cybersecurity patch makes the option to invest in cybersecurity particularly valuable under high cost uncertainty.

V. CONCLUSIONS

We develop a real options framework in order to analyse how uncertainty over (i) the cost of cyber attacks, and (ii) the arrival of cybersecurity controls impacts a firm's optimal investment strategy. We assume that the cost of cybersecurity breaches follows a GBM and that cybersecurity controls become available at random points in time according to a Poisson process. In line with Gordon *et al.* [6], our results indicate that uncertainty over the cost of cyber attacks raises the value of waiting, and, in our case, the firm's incentive to delay permanent abandonment. This result reflects the relationship between uncertainty and irreversibility, specifically that the firm would not want to terminate operations permanently due to temporary high cost that are more likely to occur when uncertainty is high. In addition, we extend the existing literature on cybersecurity investment by allowing for uncertainty over the arrival of a cybersecurity control. Specifically, we show how uncertainty over the impact of cybersecurity breaches interacts with uncertainty over the availability of cybersecurity controls to impact a firm's investment opportunity. Also, we find that the option to invest in cybersecurity increases the incentive to suspend operations temporarily in order to enhance cybersecurity, thus resuming operations when the system becomes resilient. In terms of future work, we intend to relax the assumption of risk neutrality and study how risk aversion due to technical risk affects the optimal investment policy via a utility-based framework [28]. We further aim to accommodate a different stochastic process in order to relax the limitations inherent in the GBM.

APPENDIX

A. SINGLE INSURANCE OPTION: PROOFS

The value of the option to invest and restore the efficiency of the project is indicated in (A-1). The first two terms on the top part of A-1 reflect the immediate profit.

$$F_{0,1}^{(0)}(C)=\begin{cases}(1-rdt)\mathbb{E}_C\left[F_{0,1}^{(0)}(C+dC)\right], & C>C_{0,1}^{(0)}\\ \dfrac{P\overline{D}}{r}-\dfrac{C}{r-\mu}-I, & C\le C_{0,1}^{(0)}\end{cases} \tag{A-1}$$

By expanding the top branch on the right-hand side of (A-1) using Itô's lemma, we obtain the differential equation for $F_{0,1}^{(0)}(P)$. The latter is indicated in (A-2), where $\mathcal{L}=\frac{1}{2}\sigma^2C^2\frac{\mathbf{d}^2}{\mathbf{d}C^2}+\mu C\frac{\mathbf{d}}{\mathbf{d}C}$ denotes the differential generator.

$$[\mathcal{L}-r]F_{0,1}^{(0)}(C)=0,\quad C>C_{0,1}^{(0)} \tag{A-2}$$

The solution of (A-2) for $C>C_{0,1}^{(0)}$ takes the form $A_{0,1}^{(0)}C^{\beta_2}$, and, therefore, $F_{0,1}^{(0)}(C)$ is indicated in (A-3).

$$F_{0,1}^{(0)}(C)=\begin{cases}A_{0,1}^{(0)}C^{\beta_2}, & C>C_{0,1}^{(0)}\\ \dfrac{P\overline{D}}{r}-\dfrac{C}{r-\mu}-I_1, & C\le C_{0,1}^{(0)}\end{cases} \tag{A-3}$$

The endogenous constant, $A_{0,1}^{(0)}$, and the optimal investment threshold, $C_{0,1}^{(0)*}$, are determined via the value-matching and smooth-pasting conditions between the two branches. These conditions are indicated in (A-4) and (A-5).

$$A_{0,1}^{(0)}C^{\beta_2}=\Phi_1^{(0)}(C)\Big|_{C=C_{0,1}^{(0)*}} \tag{A-4}$$

$$\beta_2A_{0,1}^{(0)}C^{\beta_2-1}=\frac{\mathbf{d}\Phi_1^{(0)}(C)}{\mathbf{d}C}\Big|_{C=C_{0,1}^{(0)*}} \tag{A-5}$$

Solving for $A_{0,1}^{(0)}$ and $C_{0,1}^{(0)*}$ we obtain the expressions indicated in (14) and (15).

Next, we step back and consider the expected value of the suspended project, (A-6).

$$\Phi_0^{(1)}(C)=\begin{cases}A_{0,1}^{(0)}C^{\beta_2}+B_0^{(1)}C^{\delta_2}, & C>C_{0,1}^{(0)}\\ \dfrac{\lambda P\overline{D}}{r(r+\lambda)}-\dfrac{\lambda C}{(r-\mu)(r+\lambda-\mu)}-\dfrac{\lambda I_1}{r+\lambda}\\ \quad+E_0^{(1)}C^{\delta_1}, & C\le C_{0,1}^{(0)}\end{cases} \tag{A-6}$$

The endogenous constants $B_0^{(1)}$ and $E_0^{(1)}$ are determined via value-matching and smooth-pasting conditions between the two branches and are indicated in (A-7) and (A-8).

$$B_0^{(1)}=\frac{{C_{0,1}^{(0)}}^{-\delta_2}}{\delta_1-\delta_2}\left[\frac{\delta_1\lambda P\overline{D}}{r(r+\lambda)}-\frac{(\delta_1-1)\lambda C_{0,1}^{(0)}}{(r-\mu)(r+\lambda-\mu)}-\frac{\delta_1\lambda I_1}{(r+\lambda)}-(\delta_1-\beta_2)A_{0,1}^{(0)}{C_{0,1}^{(0)}}^{-\beta_2}\right] \tag{A-7}$$

$$E_0^{(1)}=\frac{{C_{0,1}^{(0)}}^{-\delta_1}}{\delta_1-\delta_2}\left[\frac{\delta_2\lambda P\overline{D}}{r(r+\lambda)}-\frac{(\delta_2-1)\lambda C_{0,1}^{(0)}}{(r-\mu)(r+\lambda-\mu)}-\frac{\delta_2\lambda I_1}{(r+\lambda)}-(\delta_2-\beta_2)A_{0,1}^{(0)}{C_{0,1}^{(0)}}^{-\beta_2}\right] \tag{A-8}$$

Notice that by setting $\lambda=0$ we have $\delta_1=\beta_1$ and $\delta_2=\beta_2$. Hence, $B_0^{(1)}=\frac{C^{-\beta_2}}{\beta_1-\beta_2}\left[-(\beta_1-\beta_2)A_{0,1}^{(0)}C^{\beta_2}\right]=-A_{0,1}^{(0)}$.

Proposition 1: An embedded option to invest in a cybersecurity control accelerates abandonment, i.e., $C_{1,0}^{(1)^*}<C_{1,0}^{(0)^*}$.

Proof: The embedded option to restore the efficiency of the project to its original level raises the expected value of the investment opportunity and lowers the optimal investment threshold. Equivalently, note that compared to (11), the extra two terms on the right-hand side of (20) raise the MC of delaying suspension, thereby decreasing the marginal value of delaying suspension and increasing the incentive to suspend operations.

Proposition 2: Uncertainty over the cost of a cybersecurity breach and the arrival of a security patch raises the relative gain in option value, $\frac{F_{1,0}^{(1)}(C)-F_{1,0}^{(0)}(C)}{F_{1,0}^{(1)}(C)}$.

Proof: The maximised value of the option to abandon in the absence of a cybersecurity investment option is indicated in (A-9).

$$F_{1,0}^{(0)}(C) = \left(\frac{C}{C_{1,0}^{(0)*}}\right)^{\beta_1} \Phi_0^{(0)}\left(C_{1,0}^{(0)*}\right) \tag{A-9}$$

If the firm has a single embedded investment option, then the value of the option to suspend operation temporarily is indicated in (A-11).

$$F_{1,0}^{(1)}(C) = \left(\frac{C}{C_{1,0}^{(1)}}\right)^{\beta_1}\left[\frac{C_{1,0}^{(1)}}{r-\mu} - \frac{P\underline{D}}{r} - I_0 + \Phi_0^{(1)}\left(C_{1,0}^{(1)}\right)\right], \quad C > C_{0,1}^{(0)} \tag{A-10}$$

Notice that $F_{1,0}^{(1)}(C) = F_{1,0}^{(0)}(C)$ for $\lambda = 0$. By contrast, if $\lambda \to \infty$, then the maximised value of the option to invest is indicated in (A-11).

$$F_{1,0}^{(1)}(C) = \left(\frac{C}{C_{1,0}^{(1)}}\right)^{\beta_1}\left[\frac{C_{1,0}^{(1)}}{r-\mu} - \frac{P\underline{D}}{r} - I_0 + A_{0,1}^{(0)}C^{\beta_2}\right] \tag{A-11}$$

Consequently, for $\lambda = 0$ the relative gain in option value is zero, whereas for $\lambda \to \infty$ the relative gain in option value is indicated in (A-12).

$$\frac{F_{1,0}^{(1)}(C) - F_{1,0}^{(0)}(C)}{F_{1,0}^{(1)}(C)} = 1 - \frac{\Phi_0^{(0)}}{\Phi_0^{(1)}} \tag{A-12}$$

REFERENCES

[1] G. Martin, J. Kinross, and C. Hankin, "Effective cybersecurity is fundamental to patient safety," 2017. [Online]. Availble: http://www.bmj.com/content/357/bmj.j2375
[2] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.
[3] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Syst.*, vol. 86, pp. 13–23, Jun. 2016.
[4] Y. J. Lee, R. J. Kauffman, and R. Sougstad, "Profit-maximizing firm investments in customer information security," *Decision Support Syst.*, vol. 51, no. 4, pp. 904–920, 2011.
[5] B. Srinidhi, J. Yan, and G. K. Tayi, "Allocation of resources to cybersecurity: The effect of misalignment of interest between managers and investors," *Decision Support Syst.*, vol. 75, pp. 49–62, Jul. 2015.
[6] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Information security expenditures and real options: A wait-and-see approach," *Comput. Secur. J.*, vol. 19, no. 2, pp. 1–7, 2003.
[7] A. Pivorienė, "Real options and discounted cash flow analysis to assess strategic investment projects," *Econ. Bus.*, vol. 30, no. 1, pp. 91–101, 2017.
[8] S. Majd and R. S. Pindyck, "Time to build, option value, and investment decisions," *J. Financial Econ.*, vol. 18, no. 1, pp. 7–27, 1987.
[9] A. Dixit and R. Pindyck, *Investment Under Uncertainty*. Princeton, NJ, USA: Princeton Univ. Press, 1994.
[10] C. Gollier, D. Proult, F. Thais, and G. Walgenwitz, "Choice of nuclear power investments under price uncertainty: Valuing modularity," *Energy Econ.*, vol. 27, no. 4, pp. 667–685, 2005.
[11] N. Malchow-Møller and B. J. Thorsen, "Repeated real options: Optimal investment behaviour and a good rule of thumb," *J. Econ. Dyn. Control*, vol. 29, no. 6, pp. 1025–1041, 2005.
[12] P. M. Kort, P. Murto, and G. Pawlina, "Uncertainty and stepwise investment," *Eur. J. Oper. Res.*, vol. 202, no. 1, pp. 196–203, 2010.
[13] Y. Balcer and S. A. Lippman, "Technological expectations and adoption of improved technology," *J. Econ. Theory*, vol. 34, no. 2, pp. 292–318, 1984.
[14] S. R. Grenadier and A. M. Weiss, "Investment in technological innovations: An option pricing approach," *J. Financial Econ.*, vol. 44, no. 3, pp. 397–416, 1997.
[15] Y. H. Farzin, K. J. M. Huisman, and P. M. Kort, "Optimal timing of technology adoption," *J. Econ. Dyn. Control*, vol. 22, no. 5, pp. 779–799, 1998.
[16] U. Doraszelski, "The net present value method versus the option value of waiting: A note on Farzin, Huisman and Kort (1998)," *J. Econ. Dyn. Control*, vol. 25, no. 8, pp. 1109–1115, 2001.
[17] K. J. M. Huisman and P. M. Kort, "Strategic technology adoption taking into account future technological improvements: A real options approach," *Eur. J. Oper. Res.*, vol. 159, no. 3, pp. 705–728, 2004.
[18] R. J. Kauffman and X. Li, "Technology competition and optimal investment timing: A real options perspective," *IEEE Trans. Eng. Manag.*, vol. 52, no. 1, pp. 15–29, Feb. 2005.
[19] K. Miltersen and E. Schwartz, "Real options with uncertain maturity and competition," Nat. Bureau Econ. Res., Cambridge, MA, USA, Tech. Rep. 12990, 2007.
[20] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *J. Accounting Public Policy*, vol. 34, no. 5, pp. 509–519, 2015.
[21] M. Daneva, "Applying real options thinking to information security in networked organizations," Univ. Twente, Enschede, The Netherlands, Tech. Rep. TR-CTIT-06-11, 2006.
[22] H. S. B. Herath and T. C. Herath, "Investments in information security: A real options perspective with Bayesian postaudit," *J. Manage. Inf. Syst.*, vol. 25, no. 3, pp. 337–375, 2008.
[23] M. Benaroch, S. Shah, and M. Jeffery, "On the valuation of multistage information technology investments embedding nested real options," *J. Manage. Inf. Syst.*, vol. 23, no. 1, pp. 239–261, 2006.
[24] H. S. B. Herath and C. S. Park, "Multi-stage capital investment opportunities as compound real options," *Eng. Econ.*, vol. 47, no. 1, pp. 1–27, 2002.
[25] L. Khansa and D. Liginlal, "Valuing the flexibility of investing in security process innovations," *Eur. J. Oper. Res.*, vol. 192, no. 1, pp. 216–235, 2009.
[26] M. Benaroch, "Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision-making," *Inf. Syst. Res.*, Apr. 2017.
[27] S. Berthold and R. Böhme, "Valuating privacy with option pricing theory," in *Economics of Information Security and Privacy*. London, U.K.: Springer, 2010, pp. 187–209.
[28] M. Chronopoulos, B. De Reyck, and A. Siddiqui, "The value of capacity sizing under risk aversion and operational flexibility," *IEEE Trans. Eng. Manag.*, vol. 60, no. 2, pp. 272–288, May 2013.

MICHAIL CHRONOPOULOS received the bachelor's degree in mathematics from the the University of Ioannina, Ioannina, Greece, the M.Sc. degree in statistics from the University of Western Michigan, Kalamazoo, and the Ph.D. degree in statistics from University College London, London, U.K. He has served as a Research Fellow with the London Business School, London, and a Research Associate with the Department of Management Science and Innovation, University College London. He has also served as an Assistant Professor with the Norwegian School of Economics, Bergen, Norway. He is currently a Senior Lecturer with the University of Brighton and an Adjunct Associate Professor with the Norwegian School of Economics. His research interests include operations research, real options, game theory, mathematical finance, energy economics, and the application of financial and operational research methods for pricing financial instruments under risk aversion and competition.

EMMANOUIL PANAOUSIS received the B.Sc. degree in informatics and telecommunications from the University of Athens, Greece, in 2006, and the M.Sc. degree in computer science from the Athens University of Economics and Business, Greece, in 2008, and the Ph.D. degree in mobile communications security from Kingston University London, U.K., in 2012. He was a Senior Lecturer of cyber security and privacy with the University of Brighton, an Invited Researcher with the Imperial College, a Post-Doctoral Researcher with the Queen Mary University of London, and a Research and Development Consultant with Ubitech Technologies Ltd., Surrey Research Park. He is currently a Lecturer (Assistant Professor) with the University of Surrey, U.K., and a member of the Surrey Centre for Cyber Security, a GCHQ, which is a recognized U.K. Academic Centre of Excellence in Cyber Security Research. His research interests are in the fields of cyber security, privacy, and algorithmic decision making.

JENS GROSSKLAGS received the master's degrees in computer science, and information management and systems from UC Berkeley and the Ph.D. degree from the School of Information, UC Berkeley. His Ph.D. thesis was on economically optimal security investments. He served as a Haile Family Early Career Assistant Professor and the Director of the Security, Privacy, and Information Economics Laboratory, Pennsylvania State University. He has held invited visiting professor appointments with the Swiss Federal Institute of Technology and the IMDEA Software Institute, and held invited visiting researcher positions with EURECOM and the Copenhagen Business School. He served as a Post-Doctoral Research Associate and a Lecturer of computer science with Princeton University. He directs the Chair of Cyber Trust and is an Associate Professor with the Department of Informatics, Technical University of Munich. In his research agenda, he is studying security and networked interactions from a theoretical and practical perspective. His academic work is very cross disciplinary and utilizes analytic, empirical, and experimental methodologies. He has been involved in security and privacy policy activities, including at the FTC, DARPA, NSF, DHS, CCC, and ENISA.