Scientific Research Publishing

iBusiness, 2018, 10, 128-143
http://www.scirp.org/journal/ib
ISSN Online: 2150-4083
ISSN Print: 2150-4075

Pricing the Cost of Cybercrime—A Financial Protection Approach

Thomas Poufinas*, Nikolaos Vordonis

Department of Economics, Democritus University of Thrace, Komotini, Greece
Email: *tpoufinas@gmail.com

How to cite this paper: Poufinas, T. and Vordonis, N. (2018) Pricing the Cost of Cybercrime—A Financial Protection Approach. *iBusiness*, **10**, 128-143.
https://doi.org/10.4236/ib.2018.103008

Received: July 2, 2018
Accepted: August 13, 2018
Published: August 16, 2018

Abstract

Infrastructures, businesses, end-users and services offered in the digitally integrated environment are exposed to a wide range of risks such as denial of service, hacking, phishing, ransomware, viruses, etc. Consequently, along with their physical life, individuals and organizations have to secure their digital life as well. Digital threats may have a major economic impact both on the individuals and the society, through the direct loss of income and/or property or even an indirect reduction of the individuals' contribution back to the society and the state. The purpose of this paper is to study the effect of cyber-attacks to the economy, to price the associated cost and to recommend possible measures that internet service providers (ISPs) and policy makers can apply in order to mitigate these risks. In order to achieve that, we employ insurance (actuarial) pricing techniques to calculate the cost of cyber-attacks for an individual and for the economy of a country in total. We are therefore at the same time in place to recommend insurance coverage solutions that can assist in protecting the entity of interest from cyber risks. This resembles to the calculation of a risk premium, as the premium is calculated taking into account only the probability of occurrence of a cyber-attack and the interest rate and not any other loadings. In this context, we mimic the pricing of a policy that provides coverage for the cyber-attack, as well as the calculation of the amount that has to be set aside in order to compensate for the one-off economic loss suffered by the individual, as a result of its occurrence. Here lies our contribution to the scientific research in the field of cyber security insurance, as we employ insurance-based actuarial techniques in order to quantify the relevant loss.

Keywords

Cybercrime, Cyber-Attack, Cyber Insurance, Digital Life, Pure Premium, Protection, Economic Loss

1. Introduction

Cyber security is an increasingly important concern for citizens, businesses and policymakers [1]. This becomes gradually more intense in increasingly many countries, as societies rely already upon cyberspace to do business, purchase products and services or exchange information with others online. This trend is expected to grow further [2], towards the continuous digitization, interconnection and integration of systems and platforms. It is thus leading individuals and corporations in having a digital life and activity, composed by the logic of bits, as part of their physical life and activity, consequently making them more vulnerable to digital threats. While digitization is transforming business models and daily lives, it is also making the global economy more vulnerable to cyber-attacks. One solution is to transfer the cyber risk to a third party. This can be applied to a wide range of incidents, from individual breach occurrences, to wider losses, such as mass data breaches, ransomware (e.g. BitLocker, WannaCry) and distributed denial-of-service attacks (ddos).

The consequences of these risks, should they materialize, vary but include direct economic loss (digital assets, income, etc.), loss or theft of personal data, disclosure of sensitive data, possible reputational damage, confidentiality or integrity issues of the information under attack [3], regulatory and/or legal exposure, loss of business and industrial secrets, increased costs of doing business, etc. Nowadays, many cyber-attacks have financial motives and focus on stealing personal data or trade secrets and/or intellectual property or even the assault of a person's digital life. When a cyber-attack occurs or a digital life is lost, a series of costs may be generated and the income-generating capacity of the affected individual may impacted. This can be short term, in the case of a cyber-attack leading to a minor loss of money and/or data, and midterm or long-term, in the case of a severe cyber-attack. The latter may lead to a large economic loss and/or information and data breach; it may delete accounts and digital profiles, cause damage to certain critical assets and properties (domains, servers and files), thus increasing the associated economic loss and reputational damage.

Such an economic loss has consequences not only for the affected individual but also for the entire economic system in which he or she operates. Therefore, the challenge is to account for the costs incurred by the cyber-attack and to the means to prevent it or compensate for it (in relation to the individual, the household, the business and the state). The methodological approach introduced in this paper evaluates the aforementioned economic loss by considering the equivalent money that the individual would not have lost if he or she had not suffered the cyber-attack.

On one hand, prevention and protection can rely on education and awareness, such as the adoption of best practices regarding a person's digital life; on technological advances, such as the use of secure sites, systems and platforms, updated and legitimate software, equipment and infrastructure etc. On the other hand, it can be based on financial-insurance means, such as the accumulation of a fund which can be spent to recover from the loss caused by a cyber-attack. The

latter is of great significance as if all other means fail there needs to be a last resort fund/ account that will cover at least for the financial loss that the affected individual will have to endure. Such a fund accumulation needs to take into account the probability of the occurrence of a cyber-attack as well as the probable loss; as such it can be offered via an insurance coverage. The commercialization of such coverage can be wholesale or retail. The first one can be achieved by embedding it as a feature to the ISP contract, to the web banking account or to the digital services offered by any provider. The second one can be realized by making it available to persons or enterprises through individual sales.

Our goal is to exploit the aforementioned approach. We propose a valuation (pricing) of the loss caused by the digital threats (digital crime) to the citizens affected by these incidents through insurance oriented methods, and we explore the potential insurance coverage that is suitable for the relevant risk. The value (price) is nothing else but the burning cost of such a coverage; it can be borne either by the provider or the state in the wholesale option. This mimics the calculation of a risk premium, as the premium is calculated by taking into account only the probability of occurrence of the cyber-attack and the interest rate, without considering any other factors (expenses or loadings). It also gives an indication of the amount that needs to be set aside to cover for the one-off economic loss suffered as result of the cyber-attack. A similar approach has been followed by Dimitriou and Poufinas [4] [5] who have used actuarial pricing techniques to estimate the cost of road traffic accidents to the economy.

Our contribution to the scientific research in the field of cyber insurance includes the application of insurance-based actuarial techniques for the quantification of the loss in present terms. Such a direction has not been exploited in the past to the best of the authors' knowledge.

2. Literature Review

The existing literature regarding cyber-attacks and other forms of digital risks for individuals, households, businesses, insurance companies and policy makers focuses more on the cost-benefit analysis [6] of the alternative investments regarding optimal investment allocation. Even in the cases at which utility functions have been employed [7] this has been done in order to compare a limited number of alternatives (such as risk pooling arrangements and managed security services) to cyber insurance. No specific utility functions are constructed and no combinations of alternatives are derived.

Moreover, in practice, although it is generally accepted that insurance policies can claim a serious market share because of the entities high awareness of cyber risk and its increasing exposure to it [8], the selection of cyber insurance as a risk mitigation tool is done based on qualitative rather than quantitative criteria. In addition, a commonly accepted risk framework does not seem to be in place [9]. As mentioned earlier the market uses no specific or uniform criteria in making the decision of purchasing cyber insurance and in most of the cases the decision seems to be lost between the different executives of the company/organization

without a specific methodological approach [9]. Furthermore, the market lacks specific indicators/metrics [6] as well as the organizational maturity level to make such decisions.

In the past, proposals have been examined for the exploitation of insurance as a risk management tool, taking into account the characteristics of digital hazards and how these affect the design of appropriate insurance policies and contracts [10], as well as the viability of insurance market for complete coverage [11]. The increasing trend of occurrence of cyber-attack incidents [12] in combination with the need to comply with the new legislation [13], contributes significantly to the demand for digital security and insurance solutions [14]. Ways of benefiting through the use of insurance policies for both business and society [15] as well as approaches, standards, incentives and rewarding to increase individual protection and security [16] have been investigated. Furthermore, models providing decision making choices regarding appropriate levels of investment in security and digital insurance for organizations, which operate or exploit critical digital resources, have been examined [17].

Despite the objective difficulties, such as the absence of optimum pricing of risk premium, the lack of a uniform way of costing and investing in insurance products against digital risks [9], the calculation of exposure to digital hazards, the classification of emerging digital hazards, the lack of reliable data [18], the asymmetric information (Shetty *et al.*, 2010) and the threat of moral hazard, which do not facilitate the development of solid insurance policies and solutions, various surveys point out that the direction of digital insurance [19] can solve the issue of managing digital risk as has been proven in the past with other risk areas (health, life, vehicle, etc). Studies show that insurance increases protection on the internet [20], while there are benefits from the adoption of preventive actions to protect against cyber-attacks, contributing to cyber resilience, including the use of insurance [21].

In this paper we introduce an insurance-oriented methodological approach to estimate the cost of cyber-attacks in a given economic system. We expect to provide a more holistic approach to the cyber-attack cost estimation. A key conceptual principle of the proposed methodology is that the overall cyber-attack cost for an individual in the economy is represented by the one-off economic loss he or she may incur. This modeling approach and its outputs can assist in proper decision making, cyber resilience, insurance coverage acquisition, investment allocation and budgeting towards cyber security.

3. Research Method

We treat a cyber-attack as a digital death, *i.e.* we claim that after a cyber-attack happens the individual has no digital life any more. This is equivalent to physical death (fatality) when we examine physical life incidents. Such an approach is justified, as in the framework of this paper we make the hypothesis that any cyber-attack leads at least to the deletion of an individual's digital profile (e.g. unique virtual identity). Alternatively—but we leave this for future research—

one may allow several incidents to occur. Allowing for more cyber attacks in the life span of a person's digital life would resemble more to a physical disability or a physical illness.

We examine the economic loss arising from the realization of such an incident. We value (price) the involved cost due to cyber-attacks to the affected individuals by calculating the present value of such an economic loss, adjusted for the probability of such an event (cyber-attack) happening. This resembles the calculation of a pure insurance premium, *i.e.* the premium calculated only with the probability of the event occurring and with the interest rate, ignoring any potential loadings (expenses, etc.). As mentioned earlier, we will mimic the calculation of the burning cost of an insurance policy that provides coverage for the risk under investigation to find the aforementioned amount.

For the purposes of our research the population of interest consists of all individuals, treating their physical age as the digital equivalent of the individual's digital age. In addition, we assume that each individual of the population is able to produce one monetary unit of income, e.g. USD 1, for their entire digital life. The cost of protecting this one unit of income is the pure premium of a whole-digital-life policy, providing coverage only in case of a cyber-attack incident. We assume that the loss we examine refers to the amount that the individual has the capacity to produce during his or her entire digital life and not just the proportion for the rest of his or her digital life, *i.e.* until a cyber-attack occurs. This starts from his or her current age x until cyber death occurs. In other words, if an individual experiences a cyber-attack with an economic impact, then his or her digital life is terminated and he or she needs to recuperate the entire income he or she is able to produce in his or her lifespan (in this case the USD 1).

For our numerical application, we consider the cyber-attack incidents in Greece. We assume that: 1) The probability (or frequency)—coming from empirical data from the Hellenic Police [22] database—of a cyber-attack happening to an individual of age x is known, for each x and for each of the following years of his or her life. To estimate it, as there is no granular and detailed information available in the Hellenic Police database, except for the total number of cyber incidents per year, we use the relevant detailed data from the FBI [23] report; the latter records cyber incidents per age band, as well as the economic loss that results from these incidents. We assume that the relevant frequencies will not be very different in the two countries. 2) The interest rate curve is horizontal, set at 2%. 3) The monetary unit of income is produced at the end of each year; should a cyber-attack occur (leading to digital death), then the potential income recovery or replacement is paid at the end of the year of the incident. 4) Any monetary contribution resembling an insurance premium, so as to accumulate the necessary capital, takes place at the beginning of the year. We take a snapshot of the population of interest and thereafter study the effect of cyber-attacks on that population, assuming there are no new entries or exits apart from those that are due to digital death from a cyber-attack.

4. A Financial Protection Approach

As the cost estimation approach is based on the actuarial methodology used to price an insurance product covering fatality (digital death in our case) either lifetime or for a specific term, we introduce the relevant notation.

Let p_x denote the probability that an individual with digital life-age x (x), will attain age $x+1$, while q_x denote the probability that the individual (x) will experience a digital fatality within one year. We set ${}_n p_x$ as the probability that individual (x) lives for n years to reach age $x+n$, ${}_n q_x$ as the probability that (x) will digitally decease within the next n years, and ${}_{m/n} q_x$ as the probability that (x) will digitally decease between ages $x+m$ and $x+m+n$. We let ${}_m q_x$ be the probability that individual with digital age x, will experience a digital fatality between ages $x+m$ and $x+m+1$.

The cost of protection per USD 1 per individual is the present value of this USD 1 for each year it could be paid, adjusted for the probability that the individual suffers a digital fatality during that year due to a cyber-attack.

We denote by $A^1_{x:n|}$ the lump sum cost of the protection of USD 1 for the digital life of the individual (x). The analytical formula of the annuity, payable at the end of the year, is

$$A^1_{x:n|} = \sum_{t=0}^{n-1} {}_{t/} q_x * (1+i)^{-(t+1)} \tag{1}$$

If for each individual the total equivalent loss is I_s, then the total lump sum cost is given by

$$A^1 = \sum_{s=1}^{N} I_s * A^1_{x_s:n_s|} \tag{2}$$

If any of the individuals (users with internet connection) in the population acquires an individual insurance policy, then he or she will pay the implied commercial premium with all the applicable loadings such as taxes, expenses, profit margin, etc. Alternatively, the insurance coverage could be offered as a feature of his or her internet connection/service. In such a case the implied premium could be added on top of the periodic fee of his or her internet connection/service contract paid to/charged by the internet service provider. So for example, for each USD 1 an individual would like to protect, by not losing it in case of a cyber incident (cyber loss), the equivalent cost of an insurance coverage needs to be calculated. This insurance coverage offers essentially a financial protection in the case of a cyber-attack.

In order to demonstrate the merit of our valuation, we apply it to the cyber-crime incidents (fatalities, for the purposes of our presentation) that occurred in Greece, as officially recorded by the Hellenic Police [22] for the years 2011 to 2016, according to the Hellenic Police data. There were 2751 incidents in 2016, 2212 incidents in 2015, 2275 incidents in 2014, 1190 incidents in 2013, 3329 incidents in 2012 and 831 incidents in 2011. This yields an average of 2098 incidents for the period 2011-2016. We calculate the probability (frequency) of an individual with age x suffering a cyber-attack for each of the following m years of his or her life, which for the purpose of this paper is equivalent to his or

her digital life. We assume that the maximum age of interest, let it be ω, is 130 years of age. This assumption does not harm the validity of our calculations as the probability of survival beyond that age is practically zero.

As data per age band are not available in the Hellenic Police database, we follow the breakdown available through the FBI [23] report assuming that the relevant frequencies for the Greek population under examination will not be (very much) different. We use the population of Greece [24] and apply the proportion of individuals that suffered a cybercrime as recorded in the FBI report. We use the average of the frequencies for the years 2016 and 2017 [23] [25].

The age bands are drawn from the Hellenic Statistical Authority [24] report; these are age bands of 10 years from 0 to 79 years of age and one age band of 50 years for citizens over 80 years of age (as we assume a maximum age of 130 years old). This yields a total of 9 age bands. We assume that the incidents within each age band follow a uniform distribution. We can thus divide the population of each age band by 10 (for ages up to 79 years old) to find the number of individuals that have suffered a cyber-attack for each year of age. The total population is taken from the latest official census from the Hellenic Statistical Authority [24]; we assume that the population remains unchanged for the years under evaluation.

We apply the FBI frequencies, which are though available for a smaller number of age bands; namely under 20, 20 - 29, 30 - 39, 40 - 49, 50 - 59 and over 60. We assume also that within each of these age bands, the number of cybercrime incidents also follows a uniform distribution so that, by dividing the number incidents with the number of years of each age band we can find the incidents corresponding to each year. We can then calculate the average number of cyber-attacks (crimes) per one (1) million people per age band (in our case for the six age bands we have chosen). We then estimate the average number of cyber-attacks (crimes) per one (1) million per year, within the six age bands under investigation. This is shown in Table 1.

Table 1. Number of cyber-deaths (fatalities) due to cyber-attacks.

Age bands	GR population per age group	population per year of age (uniform distribution)	Average frequencies based on FBI metrics	Number of cyber-attacks per age band	Number of cyber-attacks per 1 M per age band	Number of cyber-attacks per 1 M per age band per annum
under 20	2,122,544.00	106,127.20	3.81%	79.90	37.64	1.88
20 - 29	1,350,868.00	135,086.80	17.47%	366.43	271.26	27.13
30 - 39	1,635,304.00	163,530.40	20.01%	419.81	256.72	25.67
40 - 49	1,581,095.00	158,109.50	19.24%	403.64	255.29	25.53
50 - 59	1,391,854.00	139,185.40	18.58%	389.80	280.06	28.01
over 60	2,734,621.00	39,066.01	20.90%	438.41	160.32	2.29
	10,816,286.00			2098.00	193.97	

Source: Author calculations based on Hellenic Statistical Authority [24], Hellenic Police [22] and FBI [23].

In order to complete our study we assess the economic loss that a cyber-attack can cause to the individual and the society/economy as a whole. Due to the lack of more refined data (time series) related to the economic loss resulting from a cyber-attack, we take into account the average cost per capita for the years 2016 and 2017 as estimated by the FBI cyber-crime incidents [23] [25], as well as the costs presented in other studies regarding digital risks (taking into account the discrepancies and the margin of error that may be present as most of these studies try to estimate the cost from the side of a business), such as Ponemon-Accenture [26], AIG [27] and Net Diligence [28]. Furthermore, following a more horizontal approach, one may assume that the cost associated with a cyber-attack equals a percentage of the GDP per capita for the duration under investigation. Under this framework, we derive an average loss (per study) of 1) ~USD 4400 per individual as officially documented from FBI 2) ~USD 3500 from Ponemon-Accenture [26]; 3) ~USD 1900 following AIG [27]; 4) ~USD 8000 as per Net Diligence [28]; 5) ~USD 3000 according to McAfee [29]; and 6) ~USD 2500 to USD 3300, if we assume that it reached a level of 15% - 20% of the GDP per capita of Greece [30].

For the purposes of our numerical application, following the aforementioned estimations, we will try to calculate the per capita average burning cost of an individual for every USD 1000 of financial protection acquired against a cyber-attack. Finding the burning cost or premium per mille of sum assured is quite common in insurance, as then the actual burning cost or premium can be found by multiplying the burning cost or premium per mille times the number of thousands of USD of sum assured purchased or sought.

Based on the above, we calculate the average (total and per individual) economic loss (costs) when such a cyber-attack occurs, as well as the amount that should be set aside to cover for these losses either from the state (as a fixed amount per year) or from an internet service provider (as insurance protection added to an internet connection contract). We apply Equations (1) and (2) to find the average cost (lump-sum) and the per capita cost for the Greek population and produce the applicable cyber-attack mortality table, shown as **Table 2** below. We denote by lx the number of individuals who live (survive) to age x and by dx the number of individuals that die at age x.

Consequently, for a loss of USD 1000 per individual, in case an authority or provider wanted to offer financial protection to the entire population of the country from cyber-crime, it would have to put aside a lump sum of USD 4,381,215.44 to cover for the losses that are anticipated to incur as a result of cyber-attacks. That is split to a charge of USD 0.41 per individual/per capita for a population of 10,816,286 people. Such an approach is simplistic in the sense that we have assumed that there exists only one internet service provider offering such a protection for USD 0.41 for every USD 1000 of financial protection. If there is more than one provider that wanted to offer such a protection, then the cost would have been split proportionally to their clientele, following the

Table 2. Cyber-attack mortality table.

Age	lx	dx	Ax	population per age (GR)
0	1,000,000.00	1.88	545.72	106,127.20
1	999,998.12	1.88	554.76	106,127.20
2	999,996.24	1.88	563.97	106,127.20
3	999,994.36	1.88	573.37	106,127.20
4	999,992.48	1.88	582.96	106,127.20
5	999,990.60	1.88	592.74	106,127.20
6	999,988.72	1.88	602.72	106,127.20
7	999,986.84	1.88	612.89	106,127.20
8	999,984.96	1.88	623.27	106,127.20
9	999,983.08	1.88	633.86	106,127.20
10	999,981.20	1.88	644.66	106,127.20
11	999,979.32	1.88	655.67	106,127.20
12	999,977.44	1.88	666.91	106,127.20
13	999,975.56	1.88	678.36	106,127.20
14	999,973.68	1.88	690.05	106,127.20
15	999,971.80	1.88	701.98	106,127.20
16	999,969.92	1.88	714.14	106,127.20
17	999,968.04	1.88	726.54	106,127.20
18	999,966.16	1.88	739.19	106,127.20
19	999,964.28	1.88	752.10	106,127.20
20	999,962.40	27.13	765.26	135,086.80
21	999,935.27	27.13	753.46	135,086.80
22	999,908.14	27.13	741.41	135,086.80
23	999,881.01	27.13	729.13	135,086.80
24	999,853.88	27.13	716.60	135,086.80
25	999,826.75	27.13	703.81	135,086.80
26	999,799.62	27.13	690.77	135,086.80
27	999,772.49	27.13	677.47	135,086.80
28	999,745.36	27.13	663.90	135,086.80
29	999,718.23	27.13	650.06	135,086.80
30	999,691.10	25.67	635.94	163,530.40
31	999,665.43	25.67	623.00	163,530.40
32	999,639.76	25.67	609.80	163,530.40
33	999,614.09	25.67	596.33	163,530.40
34	999,588.42	25.67	582.59	163,530.40
35	999,562.75	25.67	568.58	163,530.40

Continued

36	999,537.08	25.67	554.28	163,530.40
37	999,511.41	25.67	539.70	163,530.40
38	999,485.74	25.67	524.83	163,530.40
39	999,460.07	25.67	509.65	163,530.40
40	999,434.40	25.53	494.17	158,109.50
41	999,408.87	25.53	478.52	158,109.50
42	999,383.34	25.53	462.56	158,109.50
43	999,357.81	25.53	446.28	158,109.50
44	999,332.28	25.53	429.67	158,109.50
45	999,306.75	25.53	412.73	158,109.50
46	999,281.22	25.53	395.44	158,109.50
47	999,255.69	25.53	377.81	158,109.50
48	999,230.16	25.53	359.83	158,109.50
49	999,204.63	25.53	341.48	158,109.50
50	999,179.10	28.01	322.77	139,185.40
51	999,151.09	28.01	301.20	139,185.40
52	999,123.08	28.01	279.20	139,185.40
53	999,095.07	28.01	256.76	139,185.40
54	999,067.06	28.01	233.86	139,185.40
55	999,039.05	28.01	210.51	139,185.40
56	999,011.04	28.01	186.69	139,185.40
57	998,983.03	28.01	162.39	139,185.40
58	998,955.02	28.01	137.60	139,185.40
59	998,927.01	28.01	112.32	139,185.40
60	998,899.00	2.29	86.53	39,066.01
61	998,896.71	2.29	85.97	39,066.01
62	998,894.42	2.29	85.39	39,066.01
63	998,892.13	2.29	84.81	39,066.01
64	998,889.84	2.29	84.21	39,066.01
65	998,887.55	2.29	83.60	39,066.01
66	998,885.26	2.29	82.98	39,066.01
67	998,882.97	2.29	82.35	39,066.01
68	998,880.68	2.29	81.71	39,066.01
69	998,878.39	2.29	81.05	39,066.01
70	998,876.10	2.29	80.38	39,066.01
71	998,873.81	2.29	79.69	39,066.01
72	998,871.52	2.29	78.99	39,066.01

Continued

73	998,869.23	2.29	78.28	39,066.01
74	998,866.94	2.29	77.55	39,066.01
75	998,864.65	2.29	76.81	39,066.01
76	998,862.36	2.29	76.06	39,066.01
77	998,860.07	2.29	75.29	39,066.01
78	998,857.78	2.29	74.50	39,066.01
79	998,855.49	2.29	73.70	39,066.01
80	998,853.20	2.29	72.88	39,066.01
81	998,850.91	2.29	72.04	39,066.01
82	998,848.62	2.29	71.19	39,066.01
83	998,846.33	2.29	70.32	39,066.01
84	998,844.04	2.29	69.44	39,066.01
85	998,841.75	2.29	68.53	39,066.01
86	998,839.46	2.29	67.61	39,066.01
87	998,837.17	2.29	66.67	39,066.01
88	998,834.88	2.29	65.71	39,066.01
89	998,832.59	2.29	64.73	39,066.01
90	998,830.30	2.29	63.74	39,066.01
91	998,828.01	2.29	62.72	39,066.01
92	998,825.72	2.29	61.68	39,066.01
93	998,823.43	2.29	60.62	39,066.01
94	998,821.14	2.29	59.54	39,066.01
95	998,818.85	2.29	58.44	39,066.01
96	998,816.56	2.29	57.31	39,066.01
97	998,814.27	2.29	56.17	39,066.01
98	998,811.98	2.29	55.00	39,066.01
99	998,809.69	2.29	53.81	39,066.01
100	998,807.40	2.29	52.59	39,066.01
101	998,805.11	2.29	51.35	39,066.01
102	998,802.82	2.29	50.08	39,066.01
103	998,800.53	2.29	48.79	39,066.01
104	998,798.24	2.29	47.48	39,066.01
105	998,795.95	2.29	46.13	39,066.01
106	998,793.66	2.29	44.76	39,066.01
107	998,791.37	2.29	43.37	39,066.01
108	998,789.08	2.29	41.94	39,066.01
109	998,786.79	2.29	40.49	39,066.01

Continued

110	998,784.50	2.29	39.00	39,066.01
111	998,782.21	2.29	37.49	39,066.01
112	998,779.92	2.29	35.95	39,066.01
113	998,777.63	2.29	34.37	39,066.01
114	998,775.34	2.29	32.77	39,066.01
115	998,773.05	2.29	31.13	39,066.01
116	998,770.76	2.29	29.46	39,066.01
117	998,768.47	2.29	27.76	39,066.01
118	998,766.18	2.29	26.02	39,066.01
119	998,763.89	2.29	24.25	39,066.01
120	998,761.60	2.29	22.44	39,066.01
121	998,759.31	2.29	20.60	39,066.01
122	998,757.02	2.29	18.71	39,066.01
123	998,754.73	2.29	16.80	39,066.01
124	998,752.44	2.29	14.84	39,066.01
125	998,750.15	2.29	12.84	39,066.01
126	998,747.86	2.29	10.81	39,066.01
127	998,745.57	2.29	8.73	39,066.01
128	998,743.28	2.29	6.61	39,066.01
129	998,740.99	2.29	4.45	39,066.01
130	998,738.70	2.29	2.25	

Source: Author calculations based on Hellenic Statistical Authority [24], Hellenic Police [22] and FBI [24].

same approach and adjusting only for the underlying population. In addition, the cost would have to encounter the different pricing policies of the providers, taking into account the market competition, the desired profit margin, the risk appetite and other parameters that influence the commercial premium. However, if the state wanted to protect the entire population that is subject to cyber-attacks it would have to somehow provision or charge the relevant amount.

Even if the loss is assumed to be different, our approach is still valid and applicable. One simply has to put the relevant amount as input to receive the corresponding total lump sum or the individual charge. If for example we wanted to estimate the cost for the different approaches mentioned above, then that would be a total of USD 19,277,347.92 or USD 1.78 per capita for the FBI average amount of USD 4400 per individual as, which is case 1) above. We derived the total and the per capita amounts by multiplying the lump sum of USD 4,381,215.44 by 4.4 times and the USD 0.41 per individual/per capita by 4.4 times. This is because the average amount of USD 4400 per individual is 4.4 times the USD 1000 that we did our pricing for. As explained earlier, this is the

benefit of expressing the charge per mille of sum assured; the actual charge can be found by multiplying the charge per mille times the number of thousands of USD of sum assured purchased. We can extend this approach to the other cases. This yields a total of USD 15,334,254.02 or USD 1.42 per capita for the data from Ponemon-Accenture [26], which is case 2) above. This time we multiply the lump sum amount and the per capita by 3.5 as the average loss is USD 3500, which is 3.5 times USD 1000. The total amount comes up to USD 8,324,309.33 or USD 0.77 per capita for the AIG [27] data, which is case 3) above. This time we multiply the lump sum and the per capita amount by 1.9, as the average loss is USD 1900, which is 1.9 times USD 1000. In a similar manner, we get a total of USD 35,049,723.49 or USD 3.24 per capita as per the Net Diligence [28] data, which is case 4) above. For this case we multiply times 8, as the average loss of USD 8000 is 8 times USD 1000. For the data McAfee [29] we receive a total of USD 13,143,646.31 or USD 1.22 per capita (case 5) above), by multiplying the relevant amounts by 3, as USD 3000 is 3 times USD 1000. Finally, we find a total of USD 10,953,038.59 to USD 14,458,010.94 or USD 1.01 to USD 1.34 per capita if we assume that it the average loss reached a level of 15% - 20% of the GDP per capita of Greece [30], which is case 6) described above. This is derived by multiplying times 2.5 (3.3 respectively) the corresponding amounts, as USD 2500 (USD 3300 respectively) is 2.5 times (3.3 respectively) the amount of USD 1000.

Summarizing the above, we note that we introduced an insurance oriented, financial protection approach to find what would be the burning cost of protecting an income of USD 1 from a cyber-attack. We did that by assuming that a cyber-attack practically eliminates the digital life of an individual and is thus treated as a digital fatality, similar to a physical fatality. Not only did we follow a theoretical approach, but we elaborated that it can be applied also in practice. Our numerical example was applied to the cyber-attacks that we were recorded in Greece. Consequently, our population of interest was the Greek one. Considering a loss of USD 1000 per individual, we found a lump sum cost of USD 4,381,215.44 to offer financial protection to the entire population of the country from cyber-crime, so as to cover for the losses that are anticipated to incur as a result of cyber-attacks. That is split to a charge of USD 0.41 per individual for a population of 10,816,286 people, which is the population of Greece (as of the 2011 census). Our findings can be easily extended to any population and to any assumed amount of protection that is sought. They can be easily used by the state, internet service providers, financial service providers, or any other provider that offers digital services so as to embed cyber-attack protection to their product. This is we trust the significance of our contribution in the scientific research in the field.

5. Conclusions

In this paper, we assumed that a cyber-attack results in a digital fatality, meaning that one such incident can occur in a digital lifetime. In future research, we will 1) Allow more incidents to occur, which resembles more to a disability or illness

and we will mimic the relevant pricing techniques. 2) Be looking for more detailed data, in order to better model the frequency and severity of the occurrences of cyber-crime incidents and come up with additional risk parameters. 3) Assess the conditions under which it would make sense for an individual to purchase a cyber insurance coverage (as a complementary to his or her internet service contract), as well as the various coverage levels and charge approaches that can be provided.

Cyber-attacks are an important threat of an individual's digital life. In this paper, we identify the losses that result from cyber-crime incidents and calculate the amount that is needed to offer financial protection against these losses (as a lump-sum or per capita). We assume that after a cyber-attack happens the individual has no digital life any more, which is similar to his or her physical death. Therefore, the calculation resembles to that of a pure insurance premium.

The results of the paper are useful to internet service providers—as well as other providers that offer digital services—and policymakers in order to provide a better understanding of this type of risk, as well as the amount they need to provision for, should they wish to protect the citizens of a country or their clientele respectively from these risks. It may also provide guidance for the pricing of financial protection features against cyber-attacks, embedded in internet service contracts or any other service offered through a digital environment.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Adar, E., Bisogni, F., Bohme, R., Bruck, T., Cavallini, S., Christin, N., Grossklags, J., Janello, C., Kranz, J., Nowey, T., Picot, A., Pym, D., Rath, M., Schneider, R., Telang, R. and Ward, J. (2012) Economics of Security: Facing the Challenges—A Multidisciplinary Assessment. *Tech. Rep. TP*-32-12-064-*EN-N*, European Network and Information Security Agency (ENISA).

[2] World Economic Forum (2017) The Global Risks Report. https://www.weforum.org/reports/the-global-risks-report-2017

[3] Cebula, J.J. and Young, L.R. (2010) A Taxonomy of Operational Cyber Security Risks. *Technical Note CMU/SEI*-2010-*TN*-028, Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395

[4] Dimitriou, D. and Poufinas, T. (2016) Cost of Road Accident Fatalities to the Economy. *International Advances in Economic Research*, **22**, 433-445. https://doi.org/10.1007/s11294-016-9601-0

[5] Dimitriou, D. and Poufinas, T. (2017) Quantitative Financial Analysis for the Estimation of Roadaccident Costs. *International Journal of Decision Support Systems*, **2**, 260-277. https://doi.org/10.1504/IJDSS.2017.092253

[6] Meland, P., Tondel, I. and Solhaug, B. (2015) Mitigating Risk with Cyberinsurance. *IEEE Security Privacy*, **13**, 38-43. https://doi.org/10.1109/MSP.2015.137

[7] Zhao, X., Xue, L. and Whinston, A.B. (2014) Managing Interdependent Information

Security Risks: Cyber Insurance, Managed Security Services and Risk Pooling Arrangements. *Journal of Management Information Systems*, **30**, 123-152. https://doi.org/10.2753/MIS0742-1222300104

[8] Betterley, R. (2010) Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs. http://betterley.com/samples/crmm_10_nt.pdf

[9] Filkins, B., Wright, B. and Bradford, D. (2016) Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey. SANS Institute InfoSec Reading Room.

[10] Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM*, **44**, 70-75. https://doi.org/10.1145/383694.383709

[11] Bohme, R. and Schwartz, G. (2010) Modeling Cyber-Insurance: Towards a Unified Framework (Working Paper). Workshop on the Economics of Information Security, Harvard University, Cambridge.

[12] Wheatley, S., Maillart, T. and Sornette, D. (2016) The Extreme Risk of Personal Data Breaches and the Erosion of Privacy. *The European Physical Journal B*, **89**, 1-12. https://doi.org/10.1140/epjb/e2015-60754-4

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016) General Data Protection Regulation (GDPR).

[14] Majuca, P., Yurcik, W. and Kesan, P. (2006) The Evolution of Cyberinsurance. *Working Paper*. https://www.researchgate.net/publication/1958890_The_Evolution_of_Cyberinsurance

[15] Ögüt, H., Raghunathan, S. and Menon, N. (2011) Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, **31**, 497-512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

[16] Hofmann, A. and Ramaj, H. (2011) Interdependent Risk Networks: The Threat of Cyber Attack. *International Journal of Management and Decision Making*, **11**, 312-323. https://doi.org/10.1504/IJMDM.2011.043406

[17] Young, D., Lopez, J., Rice, M., Ramsey, B. and McTasney, R. (2016) A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies. *International Journal of Critical Infrastructure Protection*, **14**, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001

[18] Eling, M. and Wirfs, J. (2015) Modelling and Management of Cyber Risk. International Actuarial Association Life Section.

[19] Maillart, T. and Sornette, D. (2010) Heavy-Tailed Distribution of Cyber-Risks. *The European Physical Journal B*, **75**, 357-364. https://doi.org/10.1140/epjb/e2010-00120-8

[20] Bolot, J. and Lelarge, M. (2009) Cyber Insurance as an Incentive for Internet Security. In: Johnson, M.E., Ed., *Managing Information Risk and the Economics of Security*, Springer, New York, 269-290. https://doi.org/10.1007/978-0-387-09762-6_13

[21] Shackelford, S. and Russell, S.L. (2014) Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy. *Minnesota Journal of International Law Online*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2509428

[22] Hellenic Police. http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=70674&Itemid=1866&lang

[23] Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (2017) Internet Crime Report. https://pdf.ic3.gov/2017_IC3Report.pdf

[24] Hellenic Statistical Authority (2017) Greece in Figures. http://www.statistics.gr/en/greece-in-figures

[25] Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (2016) Internet Crime Report. https://pdf.ic3.gov/2016_IC3Report.pdf

[26] Ponemon-Accenture (2017) Cost of Cyber Crime Study. Insights on the Security Investments That Make a Difference. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[27] AIG (2016) Behind the Numbers: Key Drivers of Cyber Insurance Claims. https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-intelligence-cyber.pdf

[28] Net Diligence (2017) Cyber Claims Study. https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition-1.3.pdf

[29] McAfee (2018) Economic Impact of Cybercrime No Slowing Down. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd

[30] Hellenic Statistical Authority (2016) Per Capita Figures (Provisional Data) (1995-2016). http://www.statistics.gr/documents/20181/984194/Per+Capita+Figures++%28Provisional+Data%29+%28+1995+-+2016+%29/fbeb32ed-56c7-4d90-bec5-9c6baa3784d5?version=1.0