MILLIMAN WHITE PAPER

An epidemiological model for silent cyber accumulation risk assessment

Alexandre Boumezoued
Yousra Cherkaoui Tangi
Thomas Peyrat

Numerous studies have highlighted the importance of silent cyber risk assessment. (See, for example, PRA [Sweeney, 2019]; ACPR [ACPR, 2019]; and EIOPA (EIOPA, 2020), among others.) We present in this paper a toy portfolio inspired by Organisation for Economic Co-operation and Development (OECD) sectors data, where the interactions with the insured are modelled through a network.

We first define the portfolio's silent exposure. Then, using a business interruption scenario, we evaluate the number of infected nodes and the probable loss using epidemiological models. From this, we see that adjustments to certain parameters (the insurer's intervention capacity or the sectors in the portfolio) could reduce the overall global loss. The peaks of contamination over time are also illustrated for each sector.

As presented in Benkhalfa & Pradat, 2021, cyber risk, whether it is affirmative or not, has several characteristics that make its modelling more challenging. The accumulation of losses is one of them. We refer to silent (or non-affirmative) cyber risk when non-cyber policies don't explicitly include or exclude cyber risk in their coverages. The Mondelez case is one to cite. Mondelez is a US multinational food company that was victim of the major ransomware attack NotPetya in 2017, causing major operational difficulties. In this attack, claims amounts were USD 100 million for a cyber event on a property policy. (See Cartagena, 2020.)

In this paper we implement an epidemiological model on a network which models potential interactions of non-cyber policyholders. We use a granular approach allowing us to model each policyholder. The model can thus be easily completed with the insurer's internal information.

Modelling cyber accumulation risk

We aim to assess the potential number of infected policies and the associated losses in a cyber accumulation event in a non-cyber portfolio. For that, we use a stochastic epidemiological model spreading in a network structure.

FROM DETERMINISTIC TO STOCHASTIC EPIDEMIOLOGICAL MODELS

In the same way that a biological virus spreads through a population, potentially leading to an epidemic, malwares can generate accumulation episodes such as Wannacry or NotPetya in 2017.

Compartmental epidemiological models are adapted to describe the spread of a virus among a global population. One of the most famous is the Susceptible, Infected and Recovered (SIR) model. The simplest way to represent the evolution of the population through the three states is using an ordinary differential equation (ODE) system (the deterministic model), where "S," "I" and "R" count the number of individuals in each state, and "N" is the overall number of individuals, as shown in Figure 1.

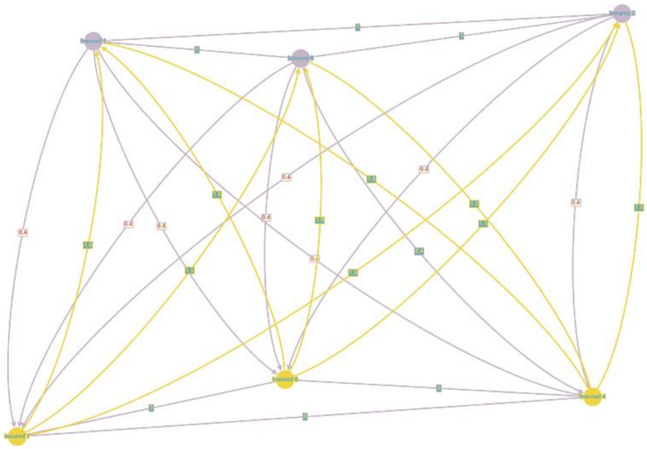
FIGURE 1: DETERMINISTIC SIR MODEL

$$\frac{dS(t)}{dt} = -\beta I(t)\frac{S(t)}{N}$$
$$\frac{dI(t)}{dt} = \beta I(t)\frac{S(t)}{N} - \gamma I(t)$$
$$\frac{dR(t)}{dt} = \gamma I(t)$$

The parameters β and γ represent, respectively, the infection and the recovery rates. As explained in Kiss, Miller & Simon, 2017, β is the rate at which infected individuals make contacts (potential infection), so the number βI represents the total number of infectious contacts. But, among all contacts made, only those in the fraction S/N are susceptible individuals.

As explained in Fahrenwaldt, Weber & Weske, 2018, a network structure within the population has a direct impact on the diffusion of the virus. The graph in Figure 2 allows us to add heterogeneity in the diffusion of viruses (in our case malwares) because their spreading speed varies according to the different classes of the population. This is achieved by using weights on the graph's edges.

FIGURE 2: EXAMPLE OF A HOMOGENEOUS WEIGHTED GRAPH FOR TWO CLASSES



As we can see, yellow edges represent the weights at which nodes from the yellow class will infect nodes from the grey class. The weighted edges within the same class represent the infection weights between nodes within the same class.

For modelling the diffusion of the virus through a network we use the continuous Markov process model. So, for N nodes $X_i \in \{S, I, R\}$ we have the following rates:

$$X_i : S \rightarrow I \; with \; rate \; \beta \sum_{j=1}^{N} a_{ij} \mathbb{1}_{\{X_j(t)= I\}}$$

$$X_i : I \rightarrow R \; with \; rate \; \gamma$$

> Where a_{ij} usually takes values in $\{0,1\}$, with 1 representing the case where a contact exists between nodes X_i and X_j and 0 the case where there is no possible contact between the two nodes. Moreover, as we want to add weights to edges, we allow a_{ij} to take values other than $\{0,1\}$.

As for the deterministic model, we can see that the recovery of an infected individual only depends on the value of γ.

The algorithm used for computing the model is the Event-Driven fast SIR described in Appendix A.1.2 of Kiss, Miller & Simon, 2017.

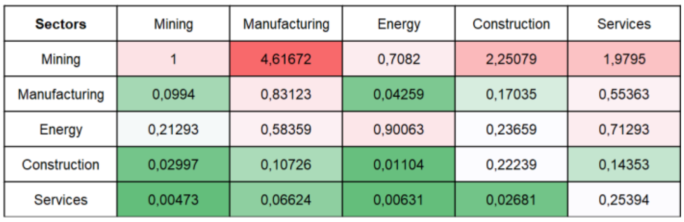
WHICH NETWORK SHOULD BE USED?

The idea behind adding a network structure to policyholders is to better reflect the environment in which the malware will spread. Furthermore, insurers will be able to determine which classes (sectors, for example) are more likely to be infected or not.

To better illustrate this, we consider the sector network introduced in Hillairet, Lopez, d'Oultremont & Spoorenbert, 2021. It is constructed using the exchanged volumes across sectors from an OECD study. We proportionate it according to one sector as a reference sector. In our modelling, the reference sector is the mining sector, meaning that the weight a_{ij} is equal to 1 if the policyholder i and the policyholder j belong to the mining sector. See the table in Figure 3.

We must keep in mind that the network structure can be calibrated using underwriting information such as partnerships, business relationships or any other relevant information. In fact, sectors could be replaced by classes representing more complex ways of quantifying connectivity among policyholders. By connectivity we mean the flow of traded added value between sectors as quantified by the OECD study. The digital connectivity is of course not reflected and would be more precise if available.

FIGURE 3: NETWORK WEIGHTS ACCORDING TO THE DIFFERENT SECTORS



Sectors	Mining	Manufacturing	Energy	Construction	Services
Mining	1	4,61672	0,7082	2,25079	1,9795
Manufacturing	0,0994	0,83123	0,04259	0,17035	0,55363
Energy	0,21293	0,58359	0,90063	0,23659	0,71293
Construction	0,02997	0,10726	0,01104	0,22239	0,14353
Services	0,00473	0,06624	0,00631	0,02681	0,25394

In the table in Figure 3 the diagonal coefficients represent the connectivity within policyholders of the same sector. The rest illustrate how members of different sectors are connected. For example, risks originating from Mining to Manufacturing are assigned weight 4.61672.

The weights presented in Figure 3 will be used for constructing the adjacency matrix of the network (i.e., the values of a_{ij}). Thus each policyholder is connected to the others but with different weights.

The matrix is not symmetric, this means that some sectors are better defended or, on the contrary, that some could be used as a vector to spread the virus.

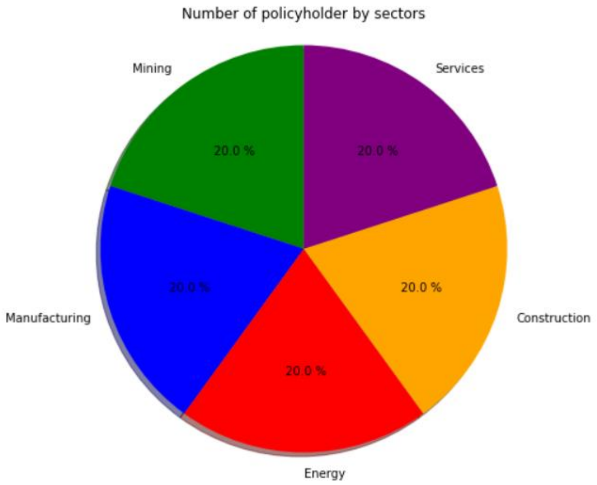
Toy portfolio

In order to study the impact of cyber accumulation threat in non-cyber framework, we consider a portfolio of professional multi-risk insurance having some heterogeneity in the policy wording due to, for example, the year of underwriting.

EACH POLICYHOLDER BELONGS TO A SECTOR

Moreover, the number of policyholders by sector is equally divided and described in Figure 4. The total number of policyholders in the toy portfolio is 1,000.

FIGURE 4: NETWORK WEIGHTS ACCORDING TO THE DIFFERENT SECTORS



USING THE EXPOSURE OF EACH POLICYHOLDER

In the toy portfolio we include the exposure for each coverage included in the policy as well as the information of the sector per insured.

By exposure we mean the difference between (if present) the sub-limit and the franchised. It is meant to represent the real compensable amount by the insurer for each coverage and each policyholder.

A substantive aspect of our modelling is to be able to quantify the silent cyber exposure.

Assessing silent exposure

We want to evaluate cyber accumulation risk in a non-cyber portfolio. To do so, we evaluate the silent exposure according to the four steps described in Figure 5. These steps are inspired by the silent cyber assessment framework of the Institute and Faculty of Actuaries (IFoA). (See Cartagena, 2020.)

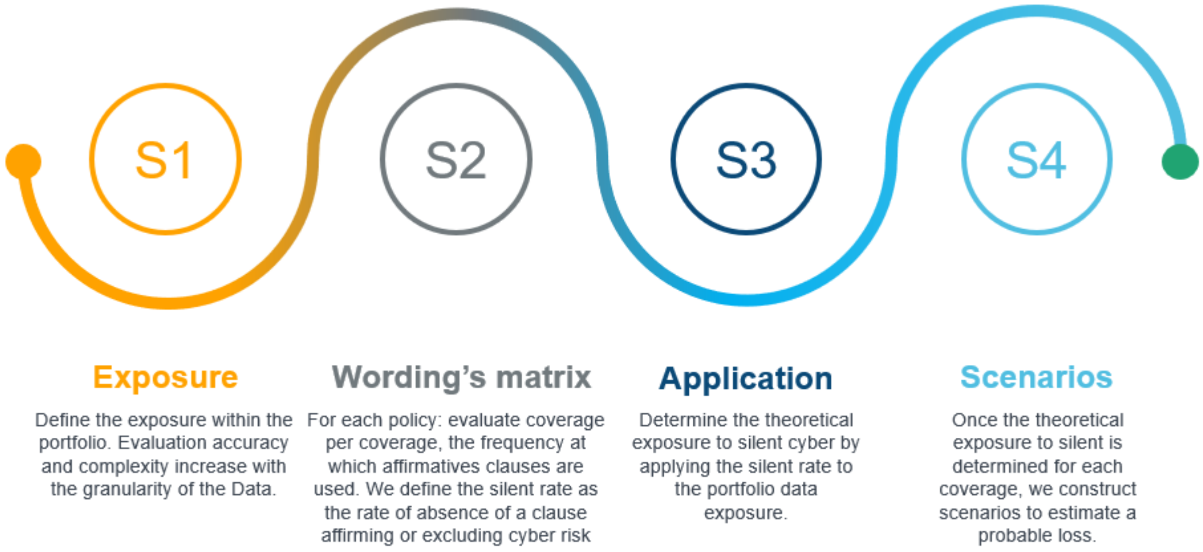
THE FOUR STEPS *ONLY* PROVIDE US SILENT EXPOSURE

The four steps of the framework illustrated in Figure 5 provide us only with the silent exposure. In our case, we aim to have the distribution of the number of the attacked nodes and the costs over time. It is the reason why we mix steps 3 and 4 with the epidemiological model presented in the first section above. To do so, each infected policyholder will activate a guarantee according to a silent rate. The guarantee represents how often a coverage misses affirmative or exclusive cyber clauses. It is determined in step 2 of Figure 5. For instance, in a professional insurance portfolio where business interruption is covered, a 20% silent rate means that, among 100 infected policyholders in our portfolio, 20 may trigger the compensation.

Evaluating the silent rate is one of the most critical parts of the modelling. Indeed, an error in the assessing will result in a wrong evaluation of the final potential loss. To better estimate this parameter, it is necessary to work with underwriting and legal services. Some features of natural language processing modelling could be used to facilitate and accelerate the estimation.

In our toy portfolio, the silent rate varies for each coverage and it is already given with the other information in the portfolio.

FIGURE 5: THE FOUR STEPS FOR ASSESSING SILENT CYBER

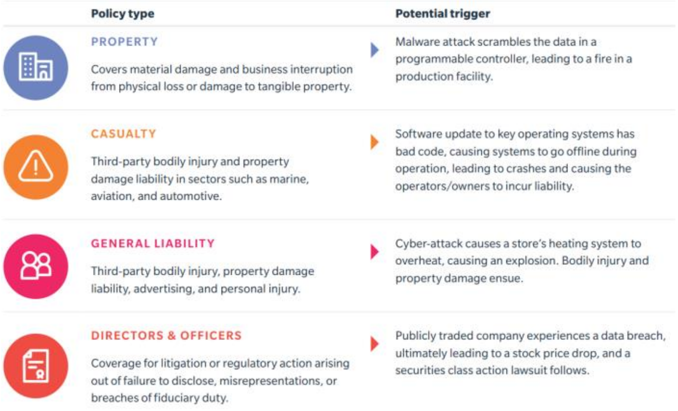

S1
S2
S3
S4
Exposure
Define the exposure within the portfolio. Evaluation accuracy and complexity increase with the granularity of the Data.
Wording's matrix
For each policy: evaluate coverage per coverage, the frequency at which affirmatives clauses are used. We define the silent rate as the rate of absence of a clause affirming or excluding cyber risk
Application
Determine the theoretical exposure to silent cyber by applying the silent rate to the portfolio data exposure.
Scenarios
Once the theoretical exposure to silent is determined for each coverage, we construct scenarios to estimate a probable loss.

Evaluating scenarios

Generating scenarios for assessing potential losses is a commonly used approach in insurance. It is used for example to assess natural disaster flooding losses.

In Figure 6, we have some examples of scenarios that could trigger silent coverages in specific policies. (See Marsh, 2020.)

FIGURE 6: THE FOUR STEPS FOR ASSESSING SILENT CYBER



Policy type	Potential trigger
PROPERTY Covers material damage and business interruption from physical loss or damage to tangible property.	Malware attack scrambles the data in a programmable controller, leading to a fire in a production facility.
CASUALTY Third-party bodily injury and property damage liability in sectors such as marine, aviation, and automotive.	Software update to key operating systems has bad code, causing systems to go offline during operation, leading to crashes and causing the operators/owners to incur liability.
GENERAL LIABILITY Third-party bodily injury, property damage liability, advertising, and personal injury.	Cyber-attack causes a store's heating system to overheat, causing an explosion. Bodily injury and property damage ensue.
DIRECTORS & OFFICERS Coverage for litigation or regulatory action arising out of failure to disclose, misrepresentations, or breaches of fiduciary duty.	Publicly traded company experiences a data breach, ultimately leading to a stock price drop, and a securities class action lawsuit follows.

In our modelling we consider that each policyholder carries a silent risk on each coverage according to the silent rate previously assessed. Hence, we define a scenario as a list of triggerable coverages. Intending to add variability to scenarios, one could link each coverage to a trigger probability.

Some realistic scenarios can be found in Lloyd's, 2022. We focus in this paper on a business interruption scenario.

Business interruption scenario

DESCRIPTION

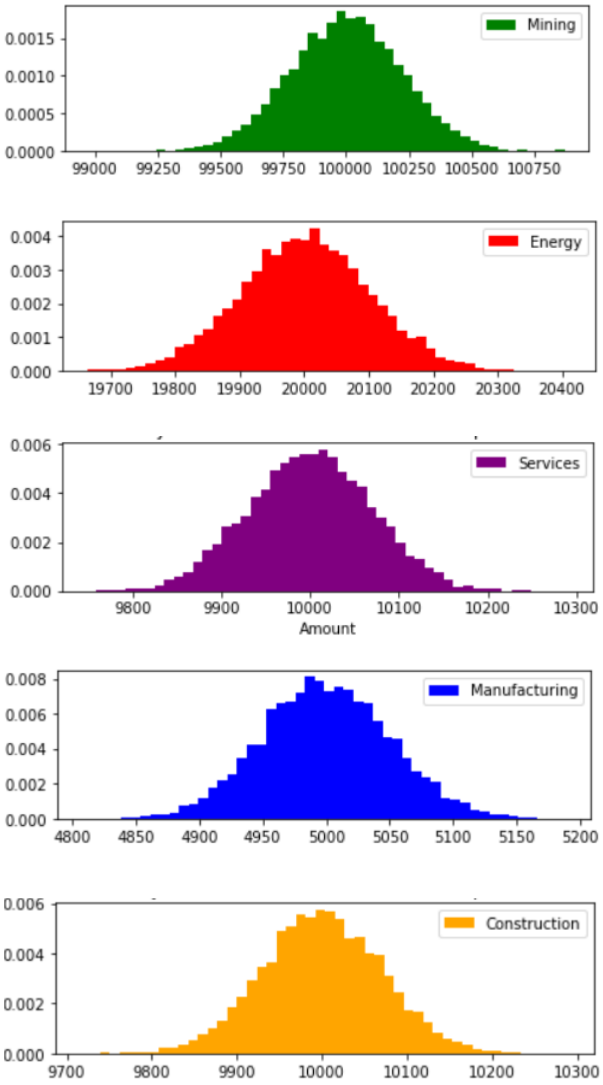
In this scenario we consider a ransomware causing a business interruption from the time of infection until the system is restored. Ransomwares are a common type of malware that encrypt data or block entire systems and restore everything once a ransom (usually in bitcoins) is paid. In this scenario we consider that the ransomware will only block the informatics system and thus cause the business interruption.

The infection parameter β (introduced in the first section above) will be fixed at 0.01 and γ, the recovery parameter, at 1. Therefore, an infected node (policyholder) will contaminate approximately 1% of the susceptible nodes it is linked to and will recover within one day. This infection percentage is subject to change due to the weighted graph we use in our model, but the recovery will not vary because it doesn't depend on the network structure.

MODELLING THE CLAIMS

We consider that the loss for one policyholder is an increasing function over the time spent paralysed by the ransomware. For each day spent in business interruption, we'll generate a random variable depending on the policyholder's sector to simulate a compensable amount. The compensable amount is truncated by the exposure marked in the portfolio meaning that the compensation can never go beyond the exposure.

FIGURE 7: DISTRIBUTION OF THE DAILY COST ACCORDING TO ITS SECTOR

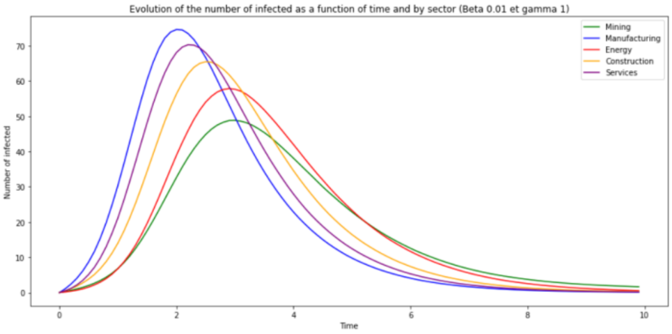


We can see in Figure 7 that the construction and services sectors have the same daily cost distribution. Furthermore, the network structure will be the one introduced in the first section above. As mentioned, because we are dealing with silent cyber not all infections lead to the activation of the business interruption coverage. In this example, the silent rate—the rate at which an infection leads to a compensation—is 32%.

RESULTS ON THE TOY PORTFOLIO

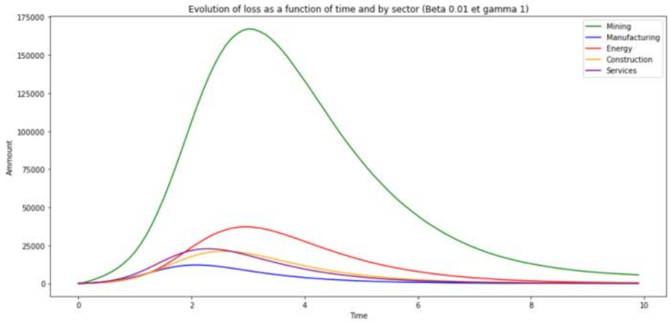
We can see in Figure 8 how the manufacturing sector is the first one to reach its infection peak. This is directly linked to the fact that manufacturing is the sector with the highest a_{ij} weight according to the mining sector. The latter infects all other sectors, as shown in the table in Figure 3 above.

FIGURE 8: NUMBER OF INFECTED PER SECTOR



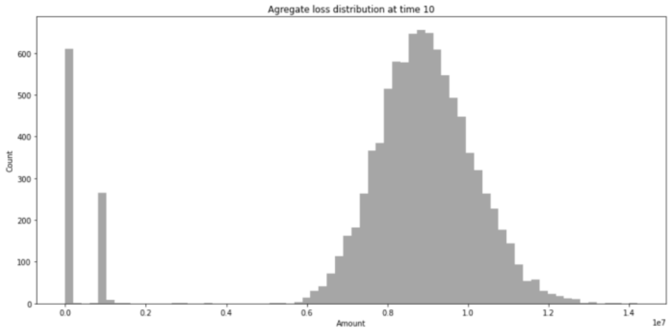
Also, we note in Figure 9 that the most exposed sector to huge daily compensations is mining. This indicates that limited contaminations (Figure 8) don't necessarily lead to reduced claims costs.

FIGURE 9: INSTANT LOSS ACROSS TIME



It is noteworthy that a stationary state exists where the malware is eradicated. In this case, no infections remain and thus no more contaminations can be generated, leading to an accumulation near to 0, as we can see in Figure 10. The latter is obtained using 10,000 simulations for up to 10 days. With these parameters and portfolio characteristics, the mean value of the cumulative loss is EUR 8,204,785.

FIGURE 10: LOSS DISTRIBUTION 10 DAYS AFTER THE INFECTION

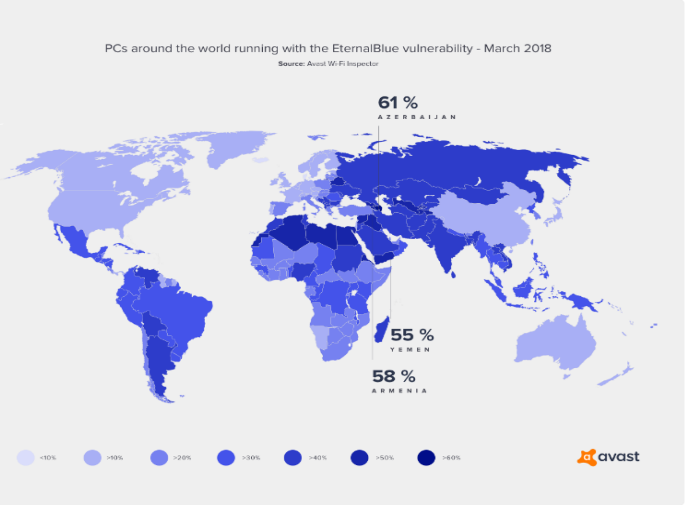


INCREASING INSURER'S "INTERVENTION" CAPACITY

Increasing the intervention capacity is modelled by increasing the recovery parameter γ. This will lead to a faster recovery of infected policyholders.

During the Wannacry cyber crisis in 2017 (see Mohurle & Patil, 2017), many Windows users were vulnerable during the crisis, and some even still one year later, even though the EternalBlue cyberattack exploit was patched (MS17-010) for Windows users in March 2017. See Figure 11.

FIGURE 11: ETERNALBLUE VULNERABILITY A YEAR AFTER WANNACRY[1]

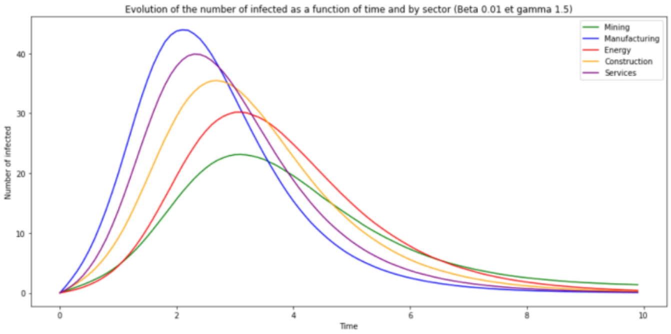

PCs around the world running with the EternalBlue vulnerability - March 2018
Source: Avast Wi-Fi Inspector
61 %
AZERBAIJAN
55 %
YEMEN
58 %
ARMENIA
<10%
>10%
>20%
>30%
>40%
>50%
>60%
avast

Some prevention measures could be implemented to enhance the insurer's intervention efficiency, such as vulnerabilities patching and greater awareness by policyholders of the system updates.

Our model does not consider prevention impacts, such as in Haillet, Lopez, d'Oultremont & Spoorenberg, 2021, where a parameter of reaction to the cyber environment is introduced, making policyholders more cautious when attacks are detected.

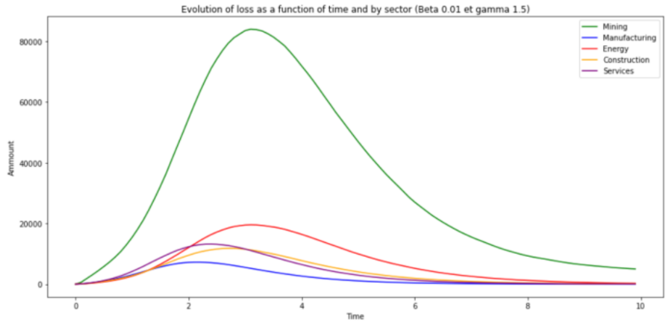
[1] Vlcek, O. (21 May 2018). WannaCry: The results one year later. Avast. Retrieved 1 March 2023 from https://blog.avast.com/fr/wannacry-le-bilan-un-an-plus-tard-avast.

FIGURE 12: NUMBER OF INFECTED PER SECTOR WITH HIGHER RECOVERY PARAMETER



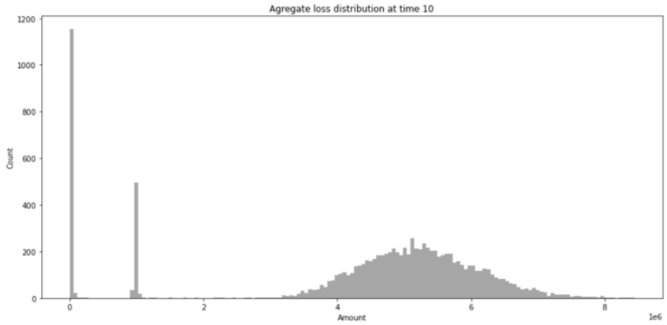
In Figure 12, we can see how increasing the recovery parameter decreases the peak of the overall paths for all sectors.

FIGURE 13: LOSS PER SECTOR WITH HIGHER RECOVERY PARAMETER



As could be expected, increasing the recovery parameters leads to less infections and thus to less costs in all sectors, as can be seen in Figure 13. Calibrating this parameter could be done using the expected recovery time, which is equal to $1/\gamma$.

FIGURE 14: LOSS DISTRIBUTION 10 DAYS AFTER THE INFECTION



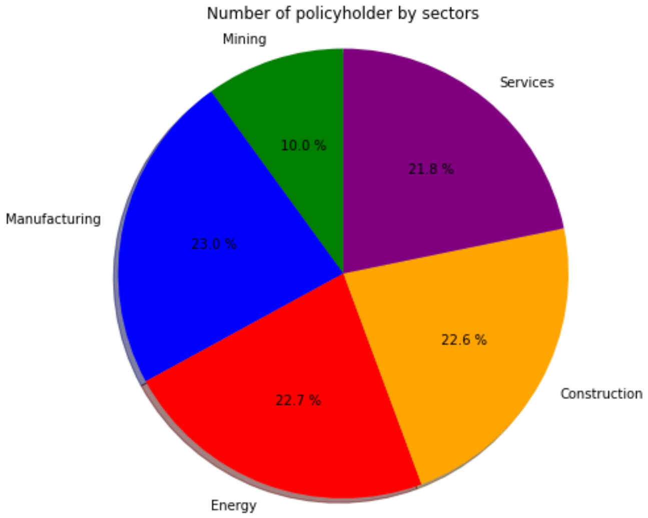
Increasing the recovery parameter might have a cost for the insurer. By adding this information, we could compare the benefits of increasing the intervention capacity against its cost. Increasing the recovery parameter γ to 1.5 allows us to decrease the overall cumulative loss by half: EUR 4,400,217.

MODIFYING THE POLICYHOLDER'S SECTOR DISTRIBUTION

In Figure 4 above, the toy portfolio has a homogeneous distribution across all sectors. But as we can see in the results in Figure 9 above, the most expensive sector is mining.

We now modify this distribution by reducing the share of the mining sector, in Figure 15. We analyse how it impacts the spread of the malware across time for each sector in Figure 16 and the associated loss in Figure 17.

FIGURE 15: NUMBER OF POLICYHOLDERS PER SECTOR



As we can see in Figure 15, the mining sector now represents only 10% of the overall sectors. This has a direct impact on the spread of the malware.

In Figure 16, the fastest contaminated sector is still manufacturing, and the slowest sector is still mining. This is due to the high contagion between mining and manufacturing (see the table in Figure 3 above). In Figure 17, the most expensive sector is energy. The diffusion's speed is conditioned by the sector.

FIGURE 16: NUMBER OF INFECTED PER SECTOR

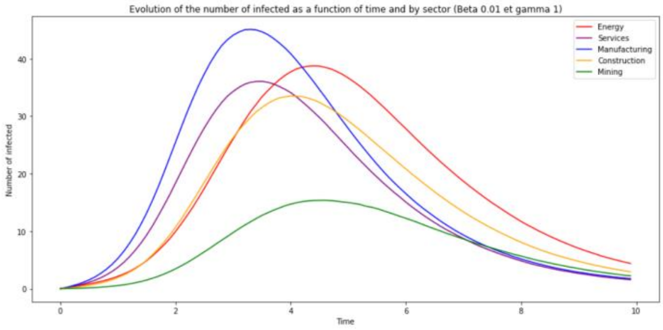
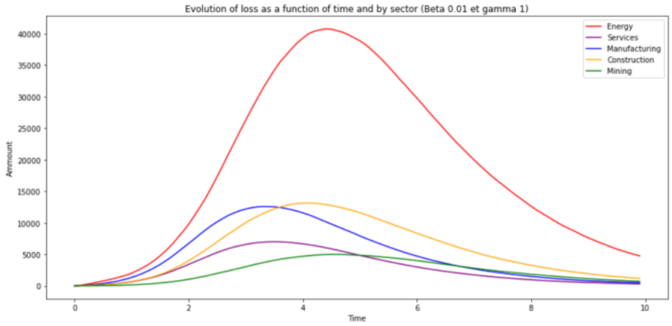
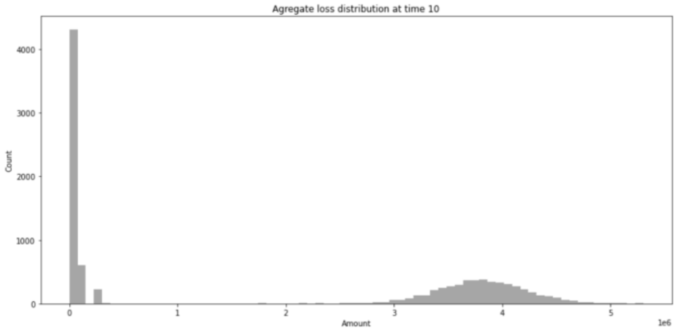


FIGURE 17: LOSS PER SECTOR ACROSS TIME



By knowing how sectors are linked, we can establish the best sector distributions for the portfolio. We are thus able to deduce some guidelines to limit the potential losses in case of a cyber accumulation scenario.

FIGURE 18: LOSS DISTRIBUTION 10 DAYS AFTER THE INFECTION



By reducing the number of mining policyholders in the portfolio, we decrease the overall loss to EUR 1,872,643. This strong decrease of the final loss is due not only to the decrease of the number of insured within the mining sector but also to the fact that the insured in this same sector are the most expensive to indemnify.

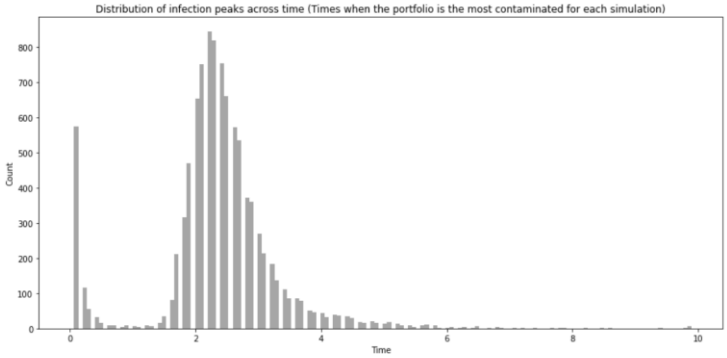
OTHER MANAGEMENT LEVERS

It is also important to recall that the loss is directly linked with the silent rate. Increasing the silent rate will automatically increase the proportion of infected policyholders who activate coverage and thus increase the overall loss.

Also, dealing with more infectious malwares will lead to a faster spreading across policyholders. The overall cumulative loss might not vary too much but might be more challenging for the insurer's solvency because the number of victims will be higher for the same time lapse.

To illustrate this, we compute the distribution of the maximum number of infections across time. This kind of information can help avoid saturation of the insurer. In Figure 19, using 10,000 simulations we can see that the average time to reach the maximum number of infections is 2.36 days for almost 800 policyholders infected per 1,000.

FIGURE 19: DISTRIBUTION OF INFECTION PEAKS ACROSS TIME FOR THE FIRST CONFIGURATION OF THE TOY PORTFOLIO PRESENTED ABOVE



Concluding remarks

In the last few years, silent cyber has been one of the big concerns in underwriting and legal services due to the complexity of its assessment.

More generally, evaluating cyber accumulation risk can be done using epidemiological models. We present in this paper a network structure that can be added to model the environment in which the virus will spread. It is the policyholder's sector in our case, but other classifications can be used to describe interactions among policyholders.

These tools not only allow us to calculate potential losses but they can also provide guidelines for insurers to better manage their provisions, portfolios and silent assessment priorities. More complex scenarios could be implemented with more underwriting information to maintain the realism of the study.

References

1. ACPR. (2019). Communiqué de presse. *La distribution des garanties contre les risques cyber par les assureurs.* Paris. Récupéré sur https://acpr.banque-france.fr/sites/default/files/medias/documents/20191112_cp_bilan_cyber_assurance.pdf

2. Benkhalfa, M., & Pradat, E. (2021, December 17). *Cyber risks: What are the challenges for insurers?* Récupéré sur https://www.milliman.com/en/insight/cyber-risks-what-are-the-challenges-for-insurers

3. Cartagena, S. G. (2020). Silent cyber assessment framework. *British Actuarial Journal*, 25. doi:10.1017/S1357321720000021

4. EIOPA. (2020). *EIOPA STRATEGY ON CYBER UNDERWRITING.* Frankfurt: EIOPA. Récupéré sur https://www.eiopa.europa.eu/sites/default/files/publications/cyber-underwriting-strategy-february-2020_0.pdf

5. Fahrenwaldt, M. A., Weber, S., & Weske, K. (2018). Pricing of Cyber Insurance Contracts in a Network Model. *ASTIN Bulletin: The Journal of the IAA*, Vol. 48, No. 3. pp. 1175-1218.

6. Hillairet, C., Lopez, O., d'Oultremont, L., & Spoorenberg, B. (2021). Cyber contagion: impact of the network structure on the losses of an insurance portfolio. *HAL open science*, 30.

7. Kiss, I. Z., Miller, J. C., & Simon, P. L. (2017). *Mathematics of Epidemics on Networks : From Exact to Approximate Models* (Vol. 1). Springer Cham: Springer Cham. doi:https://doi.org/10.1007/978-3-319-50806-1

8. Lloyd's. (2022). *Realistic Disaster Scenarios : Scenario Specification.*

9. Marsh. (2020, Septembre). "Silent Cyber" — Frequently Asked Questions.

10. Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 3. doi:https://doi.org/10.26483/ijarcs.v8i5.4021

11. Sweeney, A. (2019, January 30). *Dear CEO, Cyber underwriting risk: follow-up survey results.* Récupéré sur https://www.bankofengland.co.uk/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results

Milliman

Milliman is among the world's largest providers of actuarial, risk management, and technology solutions. Our consulting and advanced analytics capabilities encompass healthcare, property & casualty insurance, life insurance and financial services, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Alexandre Boumezoued
alexandre.boumezoued@milliman.com

Yousra Cherkaoui
yousra.cherkaoui@milliman.com