THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

CYBER

Construction of massive cyberattack scenarios: Impact of the network structure and protection measures

CAROLINE HILLAIRET | OLIVIER LOPEZ

CLOUD

#55 MAY 2022

CAPCO
a wipro company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

Editor
Shahin Shojai, Global Head, Capco Institute

Advisory Board
Michael Ethelston, Partner, Capco
Michael Pugliese, Partner, Capco
Bodo Schaefer, Partner, Capco

Editorial Board
Franklin Allen, Professor of Finance and Economics and Executive Director of the Brevan Howard Centre, Imperial College London and Professor Emeritus of Finance and Economics, the Wharton School, University of Pennsylvania
Philippe d'Arvisenet, Advisor and former Group Chief Economist, BNP Paribas
Rudi Bogni, former Chief Executive Officer, UBS Private Banking
Bruno Bonati, Former Chairman of the Non-Executive Board, Zuger Kantonalbank, and President, Landis & Gyr Foundation
Dan Breznitz, Munk Chair of Innovation Studies, University of Toronto
Urs Birchler, Professor Emeritus of Banking, University of Zurich
Géry Daeninck, former CEO, Robeco
Jean Dermine, Professor of Banking and Finance, INSEAD
Douglas W. Diamond, Merton H. Miller Distinguished Service Professor of Finance, University of Chicago
Elroy Dimson, Emeritus Professor of Finance, London Business School
Nicholas Economides, Professor of Economics, New York University
Michael Enthoven, Chairman, NL Financial Investments
José Luis Escrivá, President, The Independent Authority for Fiscal Responsibility (AIReF), Spain
George Feiger, Pro-Vice-Chancellor and Executive Dean, Aston Business School
Gregorio de Felice, Head of Research and Chief Economist, Intesa Sanpaolo
Allen Ferrell, Greenfield Professor of Securities Law, Harvard Law School
Peter Gomber, Full Professor, Chair of e-Finance, Goethe University Frankfurt
Wilfried Hauck, Managing Director, Statera Financial Management GmbH
Pierre Hillion, The de Picciotto Professor of Alternative Investments, INSEAD
Andrei A. Kirilenko, Reader in Finance, Cambridge Judge Business School, University of Cambridge
Mitchel Lenson, Former Group Chief Information Officer, Deutsche Bank
David T. Llewellyn, Professor Emeritus of Money and Banking, Loughborough University
Donald A. Marchand, Professor Emeritus of Strategy and Information Management, IMD
Colin Mayer, Peter Moores Professor of Management Studies, Oxford University
Pierpaolo Montana, Group Chief Risk Officer, Mediobanca
John Taysom, Visiting Professor of Computer Science, UCL
D. Sykes Wilford, W. Frank Hipp Distinguished Chair in Business, The Citadel

CONTENTS

CLOUD

CRYPTO

CYBER

DEAR READER,

Welcome to edition 55 of the Capco Institute Journal of Financial Transformation. Our central theme is cloud computing, which has transformed from an efficiency initiative for our clients, to an indispensable growth driver for financial services.

The pandemic has changed consumer expectations, with consumers now demanding 24/7 access to their financial resources from anywhere, as well as hyper-personalized products that reflect their lifestyle choices.

In this edition of the Journal, we explore the power of cloud and its potential applications through the lens of a joint Capco and Wipro global study, and take a deeper look at the financial services data collected in Wipro FullStride Cloud Services' 2021 Global Survey. The survey was focused on perceptions of cloud and its importance to business strategy from over 1,300 C-level executives and key decision-makers across 11 industries.

The study indicates that cloud is becoming ever more intelligent, hyperconnected, and pervasive, and enables companies to offer their end users the personalized, user-centric experience that they have come to expect. It's clear that only the financial services firms that can successfully leverage cloud, will thrive.

In addition, this edition of the Journal examines important topics around digital assets and decentralized finance, including central bank digital currencies, and bitcoin's impact on the environment, and cybersecurity and resilience.

As ever, you can expect the highest calibre of research and practical guidance from our distinguished contributors, and I trust that this will prove useful in informing your own thinking and decision-making.

Thank you to all our contributors and thank you for reading. I look forward to sharing future editions of the Journal with you.

Lance Levy, **Capco CEO**

CONSTRUCTION OF MASSIVE CYBERATTACK SCENARIOS: IMPACT OF THE NETWORK STRUCTURE AND PROTECTION MEASURES

CAROLINE HILLAIRET | Professor and Director of the Actuarial Science engineering track and Advanced Master, ENSAE and CREST
OLIVIER LOPEZ | Professor of Applied Mathematics (Statistics), Laboratoire de Probabilités, Statistique et Modélisation, Sorbonne Université[1]

ABSTRACT

This paper proposes a stochastic model to simulate massive cyberattack scenarios, taking into account the structure of the network as well as partial or full protection measures. Events, such as the recent COVID-19 pandemic, can rapidly generate consequent damages, and mutualization of the losses may not hold anymore. The framework is based on the multigroup SIR (susceptible, infected, and recovered) epidemiological model, which can be calibrated from a relatively small amount of data and through fast numerical procedures. As an illustration, we replicate the impact of a Wannacry-type event using a connectivity network inferred from macroeconomic data of the OECD. We show how this model can be used to generate reasonable scenarios of cyber events, and investigate the response to different types of attacks or behavior of the actors, allowing for the quantification of the benefits of an efficient prevention policy.

1. INTRODUCTION

With the growth of the digital economy, cyber risks are now one of the most important, if not the most important, threats facing the global financial system. The annual losses caused by cybercrime are estimated to be close to 1 percent of the world's GDP, U.S.$1 trillion. This threat has been amplified since the COVID-19 pandemic, as suggested by Kshetri (2020) and the French National Agency for Information Systems Security [ANSSI (2021)], which found a threefold increase in the number of reported ransomwares attacks between 2019 and 2020.

To face of cyber risk, insurance has a crucial role to play [Xie et al. (2020)]; and it is not only a matter of financial compensation, as cyber contracts generally include offers of prevention and assistance in the event of a loss [Romanosky et al. (2019)]. Nevertheless, quantifying the impact of this multi-faceted risk is a difficult task and a major concern for insurers. The extreme severity of some cyber events [Farkas (2021)] on the one hand and the potentially "systemic" nature of the risk on the other hand [Hillairet and Lopez (2021)] could endanger the principle of mutualization, which is at the heart of the insurance business. In particular, massive cyberattacks and contagion effects can lead to massive failures that can bring an economy to a halt, or at the very least jeopardize the solvency of an insurer. For example, the report by Cyence and Lloyd's of London [Cyence (2017)] estimates that the cost of an attack on a major cloud provider would be in the range of U.S.$15 billion to U.S.$121 billion, with an estimated average loss of U.S.$53 billion. The Wannacry or NotPetya episodes are also warning signs of massive cyberattacks, whose estimated costs are in the billions of dollars. It is important to note that even if the damages of each individual incident are low, the simultaneous occurrence of a large number of incidents in a massive attack can result in very high cumulative costs.

[1] The authors acknowledge funding from the project "Cyber Risk Insurance: actuarial modeling", Joint Research Initiative under the aegis of the Risk Foundation, in partnership with of AXA, AXA GRM, ENSAE, and Sorbonne Université.

In this paper, we propose a general and flexible framework to model the dynamics of a cyber contagion and to simulate accumulation scenarios, with a focus on their impact on an insurance portfolio. In order to take into account networks effects in the contagion [Fahrenwaldt et al. (2018)], we adopt a multi-group SIR model (susceptible, infected, and recovered) [Beretta and Capasso (1988), Guo et al. (2006), Magal et al. (2018)]. These types of compartmental models are commonly used to describe biological epidemics since McKendrick (1925), and have already been applied to several actuarial applications [Chen and Cox (2009), Lefèvre et al. (2017), Garrido and Feng (2011)]. Special attention is paid to the quantification of the impact of prevention and quick reaction to diminish the cost of such a massive cyber episode.

2. EPIDEMIOLOGICAL MODELS WITH NETWORKS EFFECTS

In order to propose a simple and flexible approach, we propose to model the strength of the cyber pandemic on the global population. Subsequently, the impact on an insurance portfolio is considered, assuming that contamination is more likely to come from outside the portfolio than from inside. This seems reasonable, based on the fact that a portfolio is in fact small when compared to the global population among which the cyber epidemic spreads.

2.1 Model on the global population

The construction of accumulation scenarios is based on stochastic epidemiological contagion models adapted to the context of cyber risk, similar to the virus contagion models like those used for the COVID-19 pandemic. Barrier measures, such as vaccinations, are replaced here by other preventive measures, such as identifying and correcting vulnerabilities. The risk of the saturation of intensive care services is replaced by the risk of being unable to provide all the necessary assistance to the insured, which could lead to an aggravation of the total costs.

Nevertheless, despite the analogy between cyber and biological epidemics, there are still differences, particularly in terms of timescales, parameter values, and the nature of the risk. Consequently, the existing models need to be adapted to the cyber context. In particular, the heterogeneity of the population (for example, in terms of security levels or of assets that can be targeted by hackers, etc.) may have an important impact on the spread of the contagion. Thus, our model relies on a multi-group SIR model (susceptible, infected, recovered) [Kermack and McKendrick (1927)]. In this model, the population is decomposed into d categories (for example, representing different sectors of activities), and the population[2] within each category $j \in [1, d]$ is split into three groups $[s_j(t), i_j(t), r_j(t))$, where for any date $t \geq 0$:

- The "**susceptibles**" [$s_j(t)$] are the entities in sector j (at date t) that can be impacted by the ongoing cyberattack.
- The "**infected**" [$i_j(t)$] are former susceptibles of sector j that became "infected" by the cybervirus and that are contagious.
- The "**removed**" [$r_j(t)$] are former infected of sector j that stopped participating in the contamination (because, for example, countermeasures have been adopted).

Then the dynamics of the population in each group is given by the following systems of ordinary differentials equations (presented in the Appendix A), where,

- The matrix $\mathbf{B} = (\beta_{k,j})_{1 \leq k,j \leq d}$ (not necessarily symmetric) conveys the information on how class k contaminates class j. This matrix is the key element of the model to capture the network topology.
- The vector $\mathbf{A}(t) = (\alpha_j(t))_{1 \leq j \leq d}$ represents a latent form of attacks (not contagious).
- The vector $\mathbf{H}(t) = (\eta_j(t))_{1 \leq j \leq d}$ represents a protection component against the threat, which diminishes the rate of new infections through time.
- The vector $\Gamma(t) = (\gamma_j(t))_{1 \leq j \leq d}$ represents the recovery rate.

By recovery, we do not mean "full recovery" (that is retrieving the same level of activity): the timescale for full recovery may be much longer than the duration of the crisis (weeks or months, compared to days). Note that this model encompasses wider situations than cyber contagion, such as, for example, a break in the supply chain (in such situations, matrix **B** generates a chain of dependence between different sectors of the activity).

At the global population level, the total number of victims from a cyber incident is computed by solving a fixed point equation whose solution can be easily determined numerically [Hillairet et al. (2021)]. Then, measuring the total number of infected individuals in each group of the population (depending on the starting point of the infection) allows us to better understand

[2] Assuming the global size of the population is constant (equal to N), which seems reasonable for a cyber crisis that only lasts a few days.

the impact of connectivity between classes and to quickly calibrate or assess the impact of such an episode.

2.2 From the multi-group SIR to the impact on an insurance portfolio

The multi-group SIR defined in Section 2.1 describes the dynamic of the cyberattack on a large population. On the other hand, an insurance portfolio is of a smaller size and can be understood as a random sample of individuals from the global population. Denoting T_m the infection date of a policyholder m (belonging to category $x_m \in [1, d]$), T_m is then a random time characterized by its hazard rate λ_{T_m} (that may be infinite):

$$\lambda_{T_m}(t) = \lim_{dt \to 0+} \frac{P(T_m \in [t, t+dt] \mid T_m \geq t)}{dt}$$

λ_{T_m} reflects the severity of the cyber-contagion at a global level, depending on the category x_m; it is given by the probability of selecting a newly infected individual among the individuals of the global population, that is

$$\lambda_{T_m}(t) = \lambda(t,j) = n_j(t)\{\alpha_j(t) + \sum_{k=1}^{d} \beta_{kj} i_k(t)\} \text{ if } x_m = j$$

Then the average number of infected policyholders of category j in the portfolio (denoting n_j the size of category j in the portfolio) is given by:

$n_j(1 - \exp\{-\int_0^\infty \lambda(t,j)dt\}) = n_j \nu_j$ with a variance of $n_j \nu_j (1 - \nu_j)$ [Hillairet et al. (2021)].

In addition to a partial protection (for example by increasing awareness of the threat) modeled through the parameter **H**, in some cases a perfect protection is possible, by implementing patches or antivirus. We model this by an independent random variable C_m that represents the time at which the policyholder m implements security changes that make them immune to the attack. As for T_m, C_m is modeled through its hazard rate λ_{C_m} and acts like a censoring-variable: denoting $\delta_m = 1_{T_m \leq C_m}$, $\delta_m = 0$ indicates that immunity has been acquired, before contamination has occurred.

The aim of this paper is to analyze the impact of the network structure and of partial or full protection measures on the spread of the attack. But before we deal with that, one important and challenging task that needs to be undertaken is calibrating the model, or at least determining reasonable numerical values for the parameters of the equations in Appendix A. We now describe the heuristic we have developed to mimic a Wannacry-type incident and its propagation, with a network structure based on OECD data.

3. NUMERICAL IMPLEMENTATION

Determining reasonable values for the parameters is a difficult task due to the lack of public data on the network structures as well as on the real-time evolution of a cyber crisis. We first consider the model in Appendix A with no reaction (that is $\eta_j = 1$ and $C_m = \infty$ for all j and all m).

3.1 Connectivity between sectors

We give an example of calibration of the network based on macroeconomic data of the OECD [OECD (2018)], to identify the dependence between some sectors of activity, namely the categories of mining, manufacturing, energy, construction, and services. Although we admit that OECD data do not provide a very accurate vision of the connectivity between these sectors, our aim is to determine a reasonable benchmark and to show that plausible parameters may be obtained through the use of a relatively small amount of data. Assuming that the digital flow between these categories is somehow proportional to the economical flow, and after a normalization by the number of companies in each category, we obtain the following connectivity matrix $\mathbf{B_0}$, with the sum of all coefficients equal to 1 [see Lopez et al. (2021) for more details on the computation of $\mathbf{B_0}$].

3.2 Simulation of a Wannacry-type event

In the dynamics described by equations in the Appendix A, we consider the contagion matrix $\mathbf{B} = \beta \mathbf{B_0}$, where parameter β captures the intensity of the contagion, is calibrated on a cyber

Table 1: Normalized connectivity matrix B_0

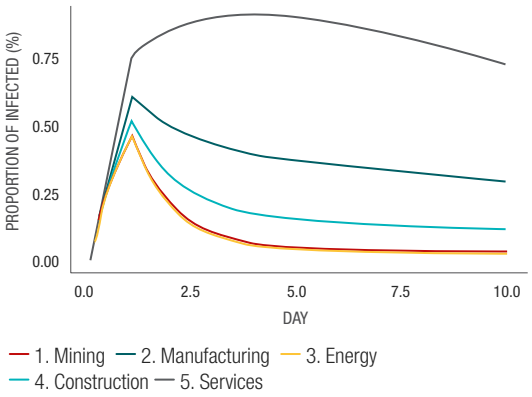
	MINING	MANUFACTURING	ENERGY	CONSTRUCTION	SERVICES	TOTAL
MINING	0.0634	0.2927	0.0449	0.1427	0.1255	0.6692
MANUFACTURING	0.0063	0.0527	0.0027	0.0108	0.0351	0.1076
ENERGY	0.0135	0.0370	0.0571	0.0150	0.0452	0.1679
CONSTRUCTION	0.0019	0.0068	0.0007	0.0141	0.0091	0.0326
SERVICES	0.0003	0.0042	0.0004	0.0017	0.0161	0.0227
TOTAL	0.0855	0.3934	0.1057	0.1844	0.2309	1

event similar to Wannacry. The Wannacry attack [May 2017, see Mohurle and Patil (2017)] is particularly emblematic due to the important number of computers infected around the world [more than 300,000 according to Chen and Bridges (2017)]. The attack consisted of a ransomware introduced into the systems through a well-documented vulnerability of Microsoft Windows [EternalBlue exploit, see Kao and Hsiao (2018)]. In this Wannacry episode, the susceptibles were computers vulnerable to the Eternal Blue exploit, but whose total number is hard to track – in fact, even the exact number of computers equipped with a given operating system is impossible to obtain. Consequently, we rely on indirect information about the total number of victims, the length of the episode (approximatively 10 days), and its dynamic (namely the timeline of the payments of ransoms, which is publicly available due to the use of the Bitcoin protocol). To ignite the epidemic, we consider a burst of infections caused by the hackers that strike the victims at uniform rate α_0 during one day: $\alpha_j(t) = \alpha_0 1_{t\leq 1}$ for all j. We take $\gamma = 1$, which corresponds to a fast containment (approximately 1 day) preventing the cyberattack to spread. This order of magnitude seems reasonable for the case of non-silent infections by malwares: once the victims identify they are attacked, links with the rest of the network may be easy to cut. This leads to the following set of parameters described in Table 2.

Table 2: Parameters used to simulate a Wannacry-type episode

PARAMETER	VALUE
α_0	7×10^{-3}
β	1.845×10^{-5}
γ	1
N	4,064,279

Figure 1: Evolution of the proportion of infected – Uniform bombing



3.3 Numerical results

We first compute the evolution through time of the infected in each category, as reported in Figure 1. We can observe that the peak of infections is not located at the same time (it is achieved later for services, with a slower decay).

We then investigate the vulnerability of the different sectors, by concentrating the initial attack on a given sector j (that is $\alpha_j(t) = \alpha^{(j)} 1_{t\leq 1}$, and $\alpha_k(t) = 0$ for $k \neq j$). To make things comparable, we take $\alpha^{(j)} = \alpha_0/p_j$, where p_j is the proportion of sector j in the global population. We compare it to the case of a uniform attack α_0 on all sectors. The proportions of companies (sector by sector) affected by the epidemic, depending on the targeted sector, are given in Table 3.

We observe that the mining sector seems to be the most contagious one. This can also make sense from a supply-chain modeling perspective. Nevertheless, this high contagiousness is to be tempered by the small population size of this sector.

4. IMPACT OF REACTIONS TO THE ATTACK

4.1 Reactions providing partial protection

We first consider the case where, during the crisis, a reaction of some categories can occur to lower the infection rate and to reduce the impact of the episode. In the Wannacry case,

Table 3: Proportion of infected sector by sector, depending on the targeted sector

TARGETED SECTOR	MINING	MANUFACTURING	ENERGY	CONSTRUCTION	SERVICES
Uniform attack	1.06%	4.11%	0.99%	2.07%	8.86%
Attack on Mining	99.70%	12.69%	1.36%	5.49%	20.37%
Attack on Manufacturing	1.02%	16.01%	0.66%	3.05%	16.58%
Attack on Energy	0.93%	5.96%	64.08%	2.35%	12.93%
Attack on Construction	0.33%	2.49%	0.21%	6.60%	5.72%
Attack on Services	0.25%	2.59%	0.21%	1.01%	7.84%

Table 4: Impact of the reaction on the number of victims

ρ = 10%	s = 10,000		s = 50,000	
	TOTAL	COLLATERAL	TOTAL	COLLATERAL
Mining	99.80%	99.99%	99,83%	99.99%
Manufacturing	94.60%	96.99%	95.82%	97.82%
Energy	99.81%	99.98%	99.84%	99.98%
Construction	98.51%	99.40%	98.87%	99.59%
Services	73.10%	77.62%	80.40%	84.36%
ρ = 50%	**s = 10,000**		**s = 50,000**	
	TOTAL	COLLATERAL	TOTAL	COLLATERAL
Mining	98.97%	99.90%	99.14%	99.93%
Manufacturing	76.87%	86.55%	81.92%	90.19%
Energy	99.03%	99.88%	99.21%	99.92%
Construction	92.99%	97.14%	94.66%	98.03%
Services	30.04%	38.29%	45.65%	54.04%

Depending on the sector which reacts (only one sector at a time) and on the thresholds activating the reaction, in case of an uniform initial attack.

for example, a "kill switch" was identified [Mohurle and Patil (2017)] that made it possible to diminish its severity. To illustrate this, we assume that the threat draws the attention of category j and is considered worth taking measures only if a sufficient number (namely s) of victims have been hit. This translates into the model presented in Appendix A, by introducing the function η_j (corresponding to the reaction of category j) given by $\eta_j(t) = 1 - \rho\, \Sigma^d_{k=1} 1_{k(t)\geq s}$.

We consider two levels of protection, $\rho = 0.1$ and $\rho = 0.5$, and two different thresholds of reaction $s = 10{,}000$ and $s = 50{,}000$. Table 4 shows the impact of reaction in case of a uniform initial attack, and when only one single sector reacts. The column "Total" shows the ratio between the number of victims if reaction, over the number of victims without reaction. The column "Collateral" shows the ratio of the number of victims in the sectors that do not react, over the number of victims in these sectors if there is no reaction at all.

One observes that the reaction having the most important impact is the one on the services sector. As this sector contains the largest number of companies, this reduction of the size of the cyber epidemic is first of all caused by the fact that fewer companies in this sector are infected, due to the reaction. But it is also interesting to notice that this induces effects in the other sectors too, since the collateral gains are quite important too.

4.2 Reactions providing full protection

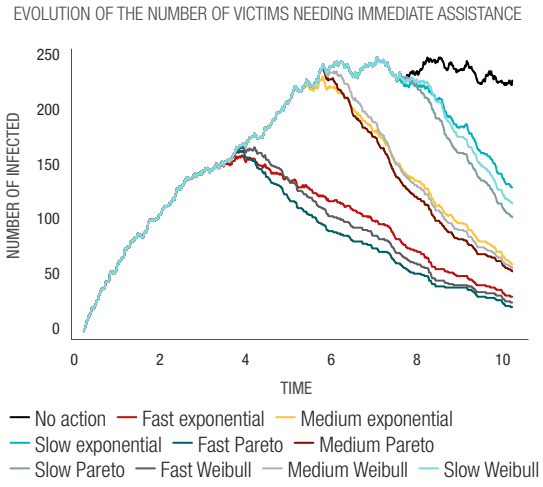
We now consider the case of an insurance portfolio of n policyholders representative of the global population. The policyholders have the possibility to implement (after some delay τ) an antivirus that provides immunity against the attack. This is captured by the random variable C (as in $\delta_m = 1_{T_m \leq C_m}$) modeled by three types of hazard rate:

- A translated exponential distribution. This means that, once the response has begun, the proportion of policyholders per time who update their security system is constant through time.
- A Pareto-type distribution. This corresponds to a situation where the vigilance of the policyholders decreases through time.
- A Weibull-type situation where there is a progressive attention devoted to this threat among policyholders.

In each case, the parameter τ represents the reactivity of the response. Figure 2 provides a simulated trajectory of the number of policyholders requiring immediate assistance, for $n = 10{,}000$ exposed policies and for three delays of reaction: a fast response ($\tau = 3$ days after the start of the event), a medium response ($\tau = 5$ days), and a slow response ($\tau = 7$ days).

The size of this peak can be of some concern, as pointed in Hillairet and Lopez (2021), since many cyber insurance contracts are supposed to provide immediate assistance to their policyholders when hit. However, a very high peak

Figure 2: Dynamics of the number of policyholders requiring immediate assistance



could lead to a situation where it might be impossible to deliver the service that was contractually guaranteed. In addition, if assistance comes too late due to saturation, this could increase significantly the amount of damages. We see that a slow response will hardly diminish the burden of the assistance teams, while a fast response in three days significantly reduces the magnitude of the peak of the attack.

5. CONCLUSION

In this paper, we propose a general and flexible model for constructing cyber-hurricane scenarios, taking into account some network structures and analyzing the impact of protection measures. In the numerical part, we use a rough connectivity matrix inferred from macroeconomic data of OECD and we mimic an event similar to the famous Wannacry episode. We emphasize the flexibility of the model, which can be easily adapted to various network structures and various scenarios. In particular, this model can be used to quantify the benefits of a reaction to such a crisis. Indeed, behavioral studies is determinant to evaluate the risk that the system collapses.

APPENDIX A: ORDINARY DIFFERENTIALS EQUATIONS MODELING THE DYNAMICS OF THE POPULATION IN EACH GROUP

$$\frac{ds_j(t)}{dt} = -\eta_j(t)\{\alpha_j(t) + \sum_{k=1}^{d}\beta_{k,j}\, i_k(t)\}s_j(t),$$
$$\frac{ds_j(t)}{dt} = \eta_j(t)\{\alpha_j(t) + \sum_{k=1}^{d}\beta_{k,j}\, i_k(t)\}s_j(t) - \gamma_i i_j(t)$$
$$\frac{dr_j(t)}{dt} = \gamma_i i_j(t)$$

REFERENCES

ANSSI, 2021, "Etat de la menace rançongiciel," Agence nationale de la sécurité des systèmes d'information, https://bit.ly/3JUq9L4

Beretta, E., and V. Capasso, 1988, "Global stability results for a multi-group SIR epidemic model," in Hallam, T. G., L. J. Gross, and S.A. Levin (eds.) Mathematical Ecology (eds.), Springer

Chen, Q., and R. A. Bridges, 2017, "Automated behavioral analysis of malware: A case study of Wannacry ransomware," 16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 454–460

Chen, H., and S. H. Cox, 2009, "An option-based operational risk management model for pandemics," North American Actuarial Journal 13:1, 54–76

Cyence, 2017, "Counting the cost – cyber-exposure decoded," https://bit.ly/3tpIQ2K

Farkas, S., O. Lopez, and M. Thomas, 2021, "Cyber claim analysis using generalized pareto regression trees with applications to insurance," Insurance: Mathematics and Economics 98, 92–105

Fahrenwaldt, M. A., S. Weber, and K. Weske, 2018, "Pricing of cyber insurance contracts in a network model," ASTIN Bulletin: The Journal of the IAA 48:3, 1175–1218

Garrido, J., and R. Feng, 2011, "Actuarial applications of epidemiological models," North American Actuarial Journal 15:1, 112–136

Guo, H., M. Y. Li, and Z. Shuai, 2006, "Global stability of the endemic equilibrium of multigroup SIR epidemic models," Canadian applied mathematics quarterly 14:3, 259–284

Hillairet, C., and O. Lopez, 2021, "Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models," Scandinavian Actuarial Journal 6, 1–24

Hillairet, C., O. Lopez, L. d'Oultremont, and B. Spoorenberg, 2021, "Cyber contagion: impact of the network structure on the losses of an insurance portfolio," working paper, https://bit.ly/35mPyhH

Kao, D.-Y., and S.-C. Hsiao, 2018, "The dynamic analysis of Wannacry ransomware," 20th International conference on advanced communication technology (ICACT), pp. 159–166. IEEE

Kermack, W. O., and A. G. McKendrick, 1927, "A contribution to the mathematical theory of epidemics," Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character 115:772, 700-721

Kshetri, N., 2020, "The evolution of cyber-insurance industry and market: an institutional analysis," Telecommunications Policy 44:8, 102007

Lopez, O., L. d'Oultremont, and B. Spoorenberg, 2021, "Modeling accumulation scenarios in cyber risk," Detra Note, Detralytics, https://bit.ly/3C2UdRN

Lefèvre, C., P. Picard, and M. Simon, 2017, "Epidemic risk and insurance coverage," Journal of Applied Probability 54:1, 286–303

Magal, P., O. Seydi, and G. Webb, 2018, "Final size of a multi-group SIR epidemic model: irreducible and non-irreducible modes of transmission," Mathematical biosciences 301, 59–67

McKendrick, A. G., 1925, "Applications of mathematics to medical problems," Proceedings of the Edinburgh Mathematical Society 44, 98–130

Mohurle, S., and M. Patil, 2017, "A brief study of Wannacry threat: ransomware attack 2017," International Journal of Advanced Research in Computer Science 8:5, 1938–1940

OECD, 2018, "Origin of value added in final demand," https://bit.ly/3tfLoAo

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones, 2019, "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity 5:1

Xie, X., C. Lee, and M. Eling, 2020, "Cyber insurance offering and performance: an analysis of the US cyber insurance market," The Geneva Papers on Risk and Insurance-Issues and Practice 45:4, 690–736

© 2022 The Capital Markets Company (UK) Limited. All rights reserved.

This document was produced for information purposes only and is for the exclusive use of the recipient.

This publication has been prepared for general guidance purposes, and is indicative and subject to change. It does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (whether express or implied) is given as to the accuracy or completeness of the information contained in this publication and The Capital Markets Company BVBA and its affiliated companies globally (collectively "Capco") does not, to the extent permissible by law, assume any liability or duty of care for any consequences of the acts or omissions of those relying on information contained in this publication, or for any decision taken based upon it.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C001648

WWW.CAPCO.COM

CAPCO
a wipro company