INFORMATION SECURITY GROUP SEMINAR

19 NOVEMBER 2020

Cyber-insurance: What is the right price?

Henry Skeoch

UCL Centre for Doctoral Training in Cyber-Security

Myths

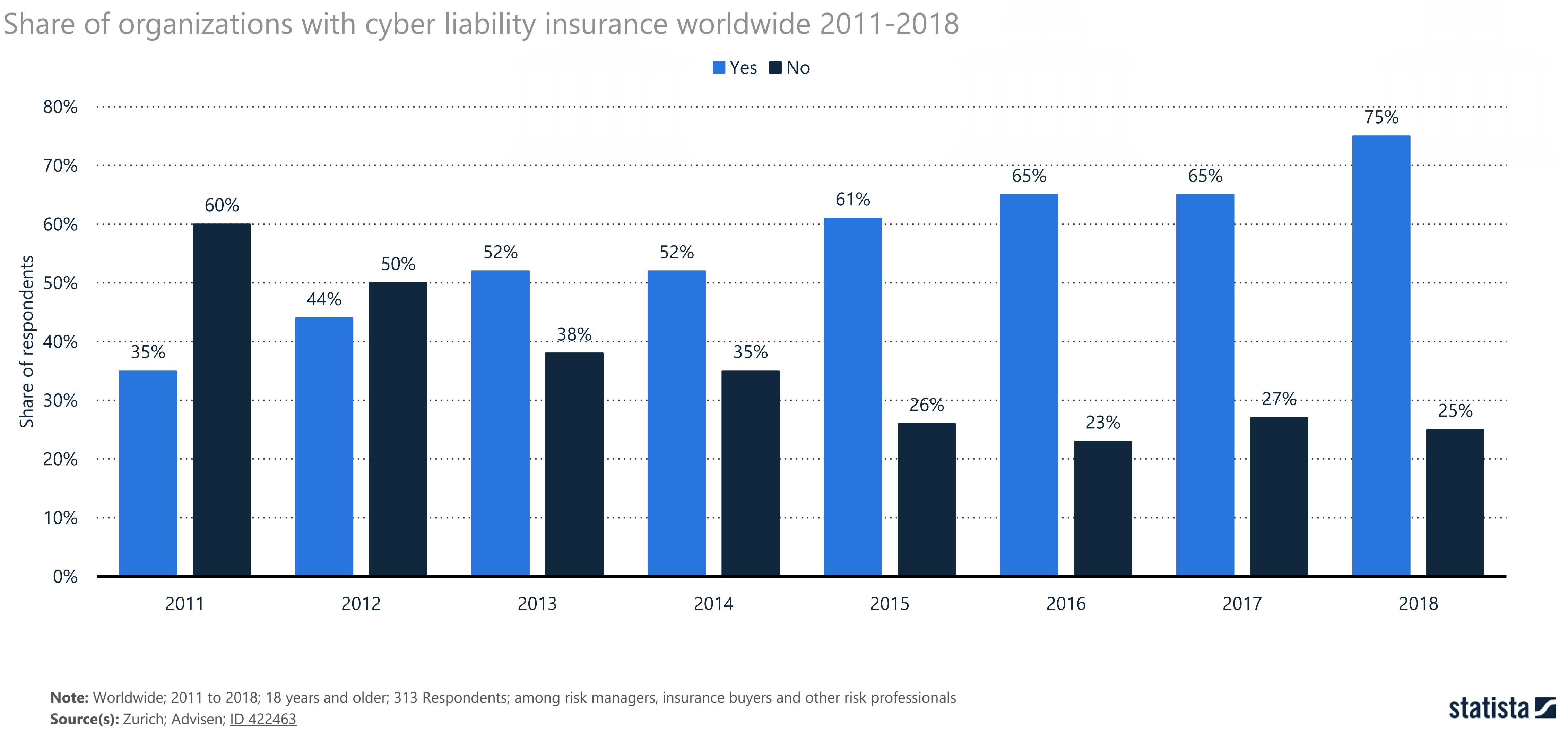
Cyber-insurance won't pay out if I'm attacked….

If the attack comes from a nation state, the insurer might claim it's an act of war…

We invest heavily in security, we don't need cyber-insurance…

Reality

Does your organization purchase cyber liability insurance?



What is Cyber-Insurance?

"Cyber insurance covers the losses relating to damage to, or loss of information from, IT systems and networks" (Association of British Insurers)

First-party insurance

- Loss or damage to digital assets
- Business interruption
- Cyber exhortation
- Customer notification expenses
- Reputational damage
- Theft of money or digital assets

Third-party insurance

- Investigative or defensive costs associated with security and privacy breaches
- Multi-media liability (e.g. breach of privacy or negligence in publication in electronic or print media)
- Loss of third-party data

Adapted from the Association of British Insurers

The field as it stands…

Insurance Economics

- Well-established
- Spans a vast array of different types of insurance products
- Theory of the demand and supply sides of insurance very well developed and studied.

+

Information Security Economics

- Relatively new
- Saw strong growth in the early 2000s
- Seminal early contribution was the Gordon & Loeb model (plenty on this in due course)

=

Cyber-Insurance

- Research coverage is sparse and the current body of literature is not cohesive
- Discipline needs structure and rigour to move forward
- Partnership between industry and academia is crucial

What are the barriers to research in Cyber-Insurance?

- Lack of actuarial data
- Little commercial advantage to providers sharing data
- Constantly evolving nature of the threat landscape
- Presented as a unified product to the customer, but actually typically an amalgamation of existing product lines

Three good papers on cyber-insurance, which navigate these issues
Romanosky et al (2017)
https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/06/WEIS_2017_paper_28.pdf
Woods et al (2017)
http://dx.doi.org/10.1186/s13174-017-0059-y
Nurse et al (2020)
https://kar.kent.ac.uk/80965/

The Gordon and Loeb Model

- Published as "The Economics of Information Security Investment" ~ TISSEC (2002)
- Introduces the concept of a security breach function S(z,v) where z is investment and v vulnerability, with three assumptions:

  A1: $S(z, 0) = 0$ for all z

  A2: For all v, $S(0, v) = v$

  A3: For all $v \in (0, 1)$ and all z, $S_z(z, v) < 0$ and $S_{zz}(z, v) > 0$ where S_z and S_{zz} are the first and second partial derivatives of the security breach probability function with respect to z.

- Key parameters of an information set are the vulnerability, v; the loss conditioned on a breach occurring, l; and probability of a threat occurring, τ. The expected loss is then:

$$E[L] = \tau v l$$

The key output we are interested in is the expected net benefit of investment in information security, ENBIS:

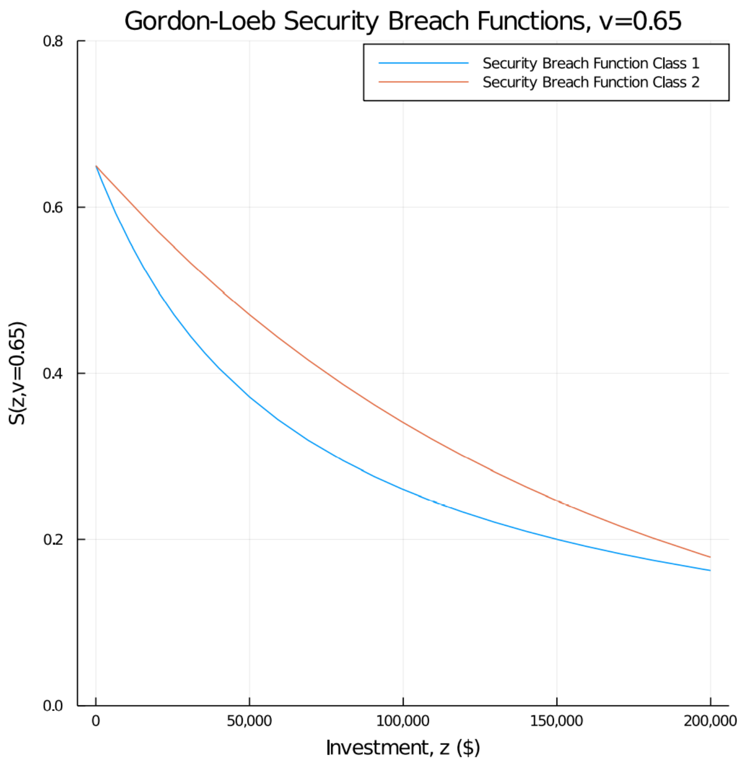
$$ENBIS(z) = [v - S(z, v)]\tau l - z$$

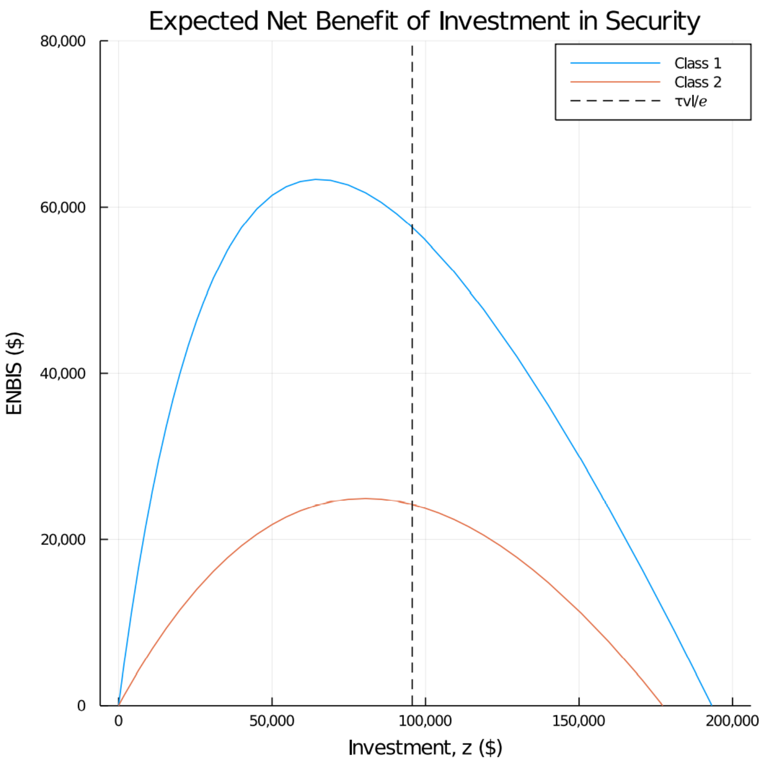
Gordon-Loeb Security Breach functions

- Two Security Breach functions proposed in the original paper:

$$S^{I}(z, v) = \frac{v}{(az+1)^{\beta}} \qquad S^{II}(a, v) = v^{\alpha z+1}$$

- A key result of the Gordon-Loeb model is that for both these forms: $z^{*}(v) < (1/e)v\tau l$





How can the Gordon-Loeb Model be expanded to cyber-insurance?

- Consider a two-state model, loss or no loss…

$$E[U] = (1 - S(v,z))u(B_{sec} - z - P(C)) + S(z,v)u(B_{sec} - z - P(C) - \tau l S(z,v) + C)$$

- P is premium, C is cover, B is budget. If we express P as a percentage of cover (p) and adding the constraint that the combination of investment and insurance bought CANNOT exceed the Gordon-Loeb limit, then formally:

$$z + pC \leq \frac{v\tau l}{e}$$

- This constraint then yields the optimisation problem:

$$\bar{u}(C,z) = (1 - S(v,z))u(B_{sec} - z - pC) + S(z,v)u(B_{sec} - z - \tau l S(z,v) + C(1-p))$$

- This can be solved via the use of a Lagrangian:

$$Z = U + \lambda(\frac{v\tau l}{e} - pC - z)$$

- The Kuhn-Tucker (i.e. first-order) conditions resulting are:

$$\begin{aligned} Z_C = U_C - p\lambda \leq 0 \qquad & C \geq 0 \qquad & C.Z_C = 0 \\ Z_z = U_z - \lambda \leq 0 \qquad & z \geq 0 \qquad & z.Z_z = 0 \\ Z_\lambda = \frac{v\tau l}{e} - pC - z \geq 0 \qquad & \lambda \geq 0 \qquad & \lambda.Z_\lambda = 0 \end{aligned}$$

A quick primer in economic utility

- Key contribution was the work by Von Neumann and Morgenstern in the 1940s, which broadly states that under axioms of rational behaviour, a decision maker faced with a risky problem will behave as if they are maximising the expected value of a function defined over potential outcomes.
- We focus on functions with constant absolute risk aversion (CARA):

$$u(z) = \frac{1 - e^{-az}}{a}$$

- And also constant relative risk aversion (CRRA):

$$u(z) = \begin{cases} z^{(1-\gamma)}/(1-\gamma) & \text{if } \gamma \neq 1 \\ ln(z) & \text{if } \gamma = 1 \end{cases}$$

$$A(z) = -\frac{u''(z)}{u'(z)}$$

$$R(z) = \frac{-zu''(z)}{u'(z)} = zA(z)$$

Key simulation parameters

$$\alpha = 1.5 * 10^{-5}$$
$$\beta = 1$$

Gordon-Loeb Security Breach Function Parameters

$$l = \$500{,}000$$
$$\tau = 0.8$$

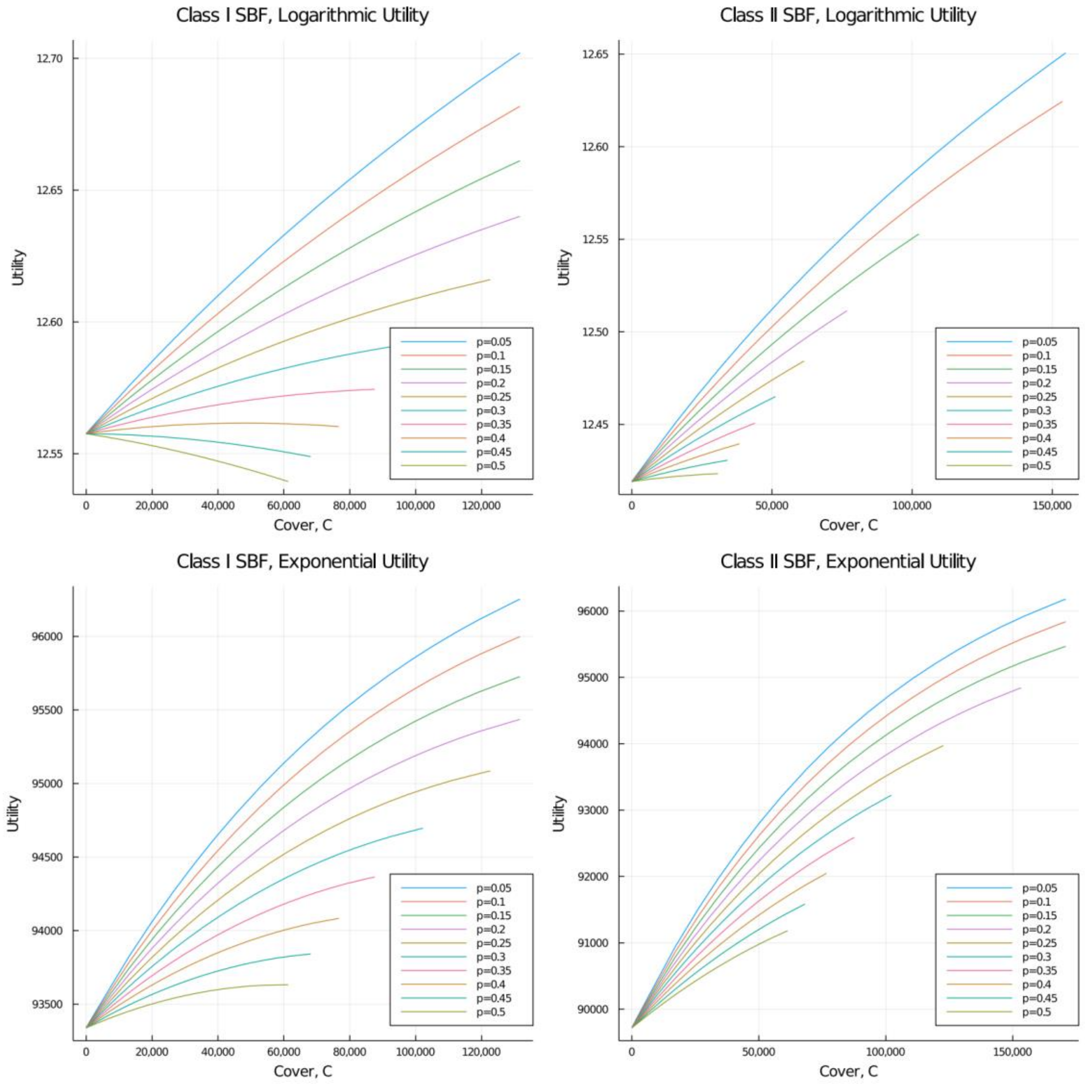
Properties of the dataset, which are fixed in the Gordon-Loeb model

$$a = 10^{-5}$$

Coefficient for the utility functions

The vulnerability v, is initially fixed at 0.65 and then this assumption is relaxed. Recall that z is the investment and z* is the optimal investment recommended by the Gordon-Loeb model.

Optimal investment, variable cover



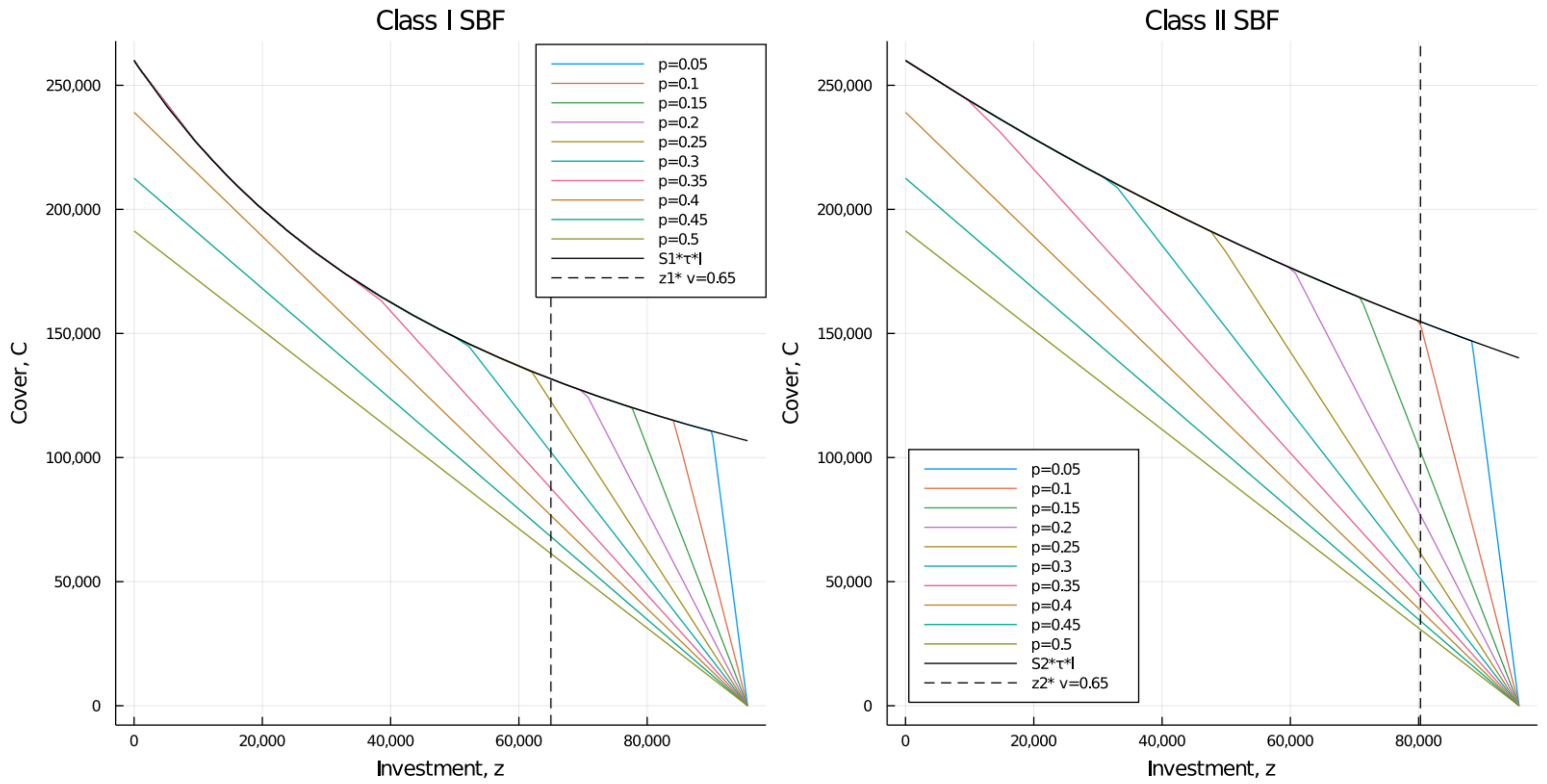
- Maximum cover to respect the Gordon-Loeb cash constraint:

$$min(\tau l S(v, z^*), \frac{(1/e)\tau v l - z^*}{p})$$

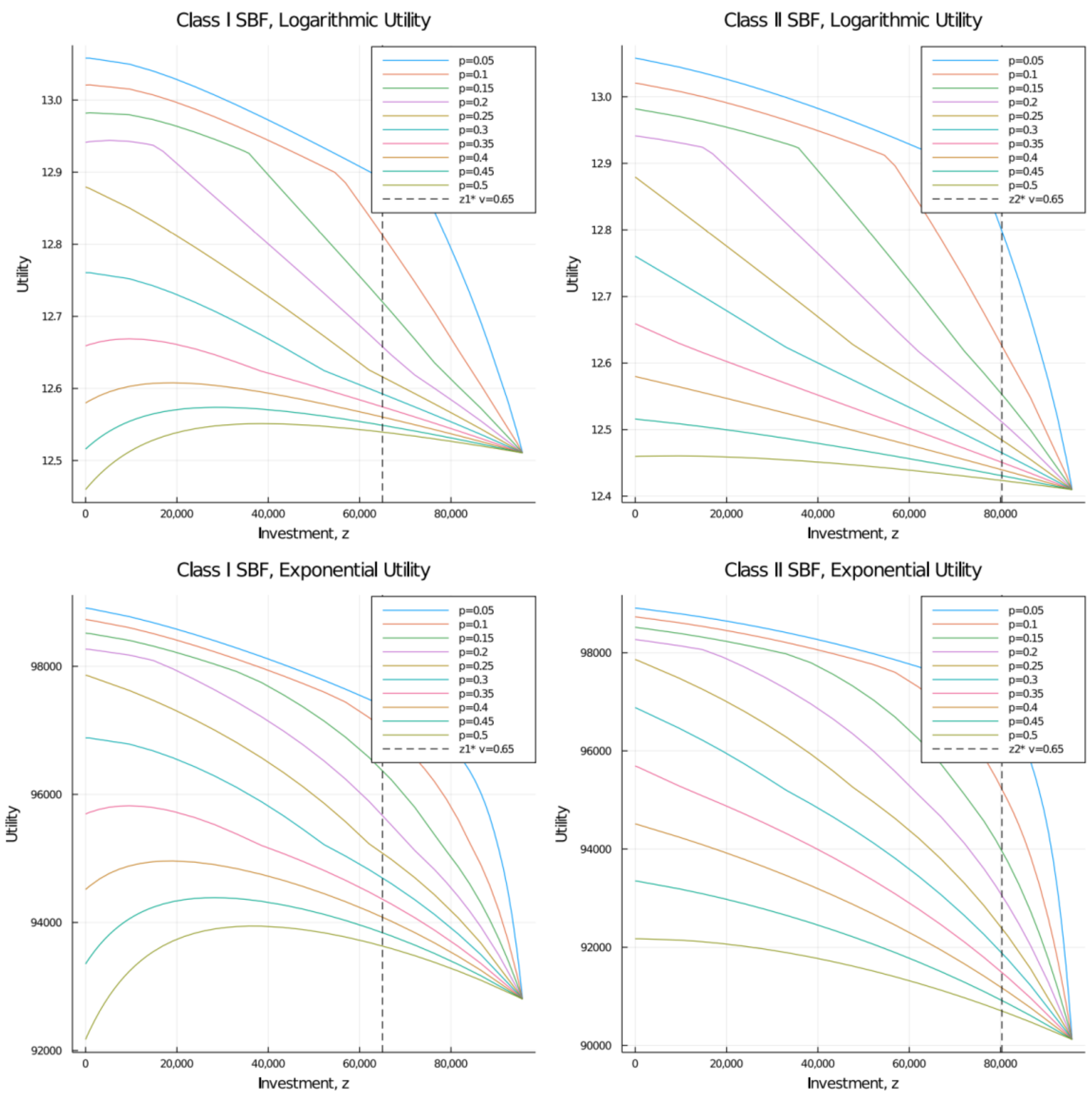
- Results suggest that utility is generally maximised at maximum insurance coverage with the assumption of defensive investment of z* recommended by the Gordon-Loeb model.

Variable Investment, maximum cover (part 1)

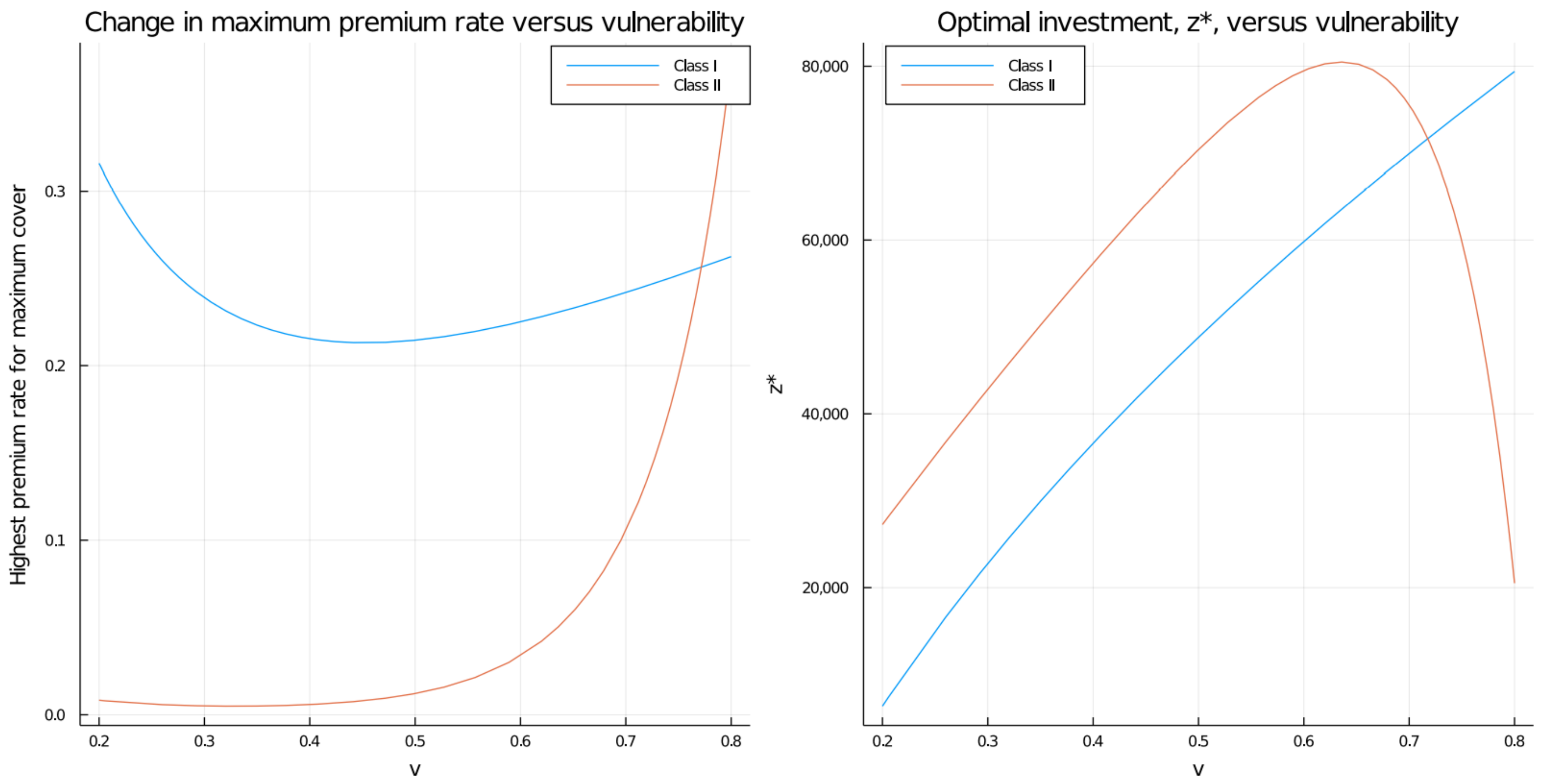
Maximum available cover under the cash constraint at different levels of z



Variable Investment, maximum cover (part 2)



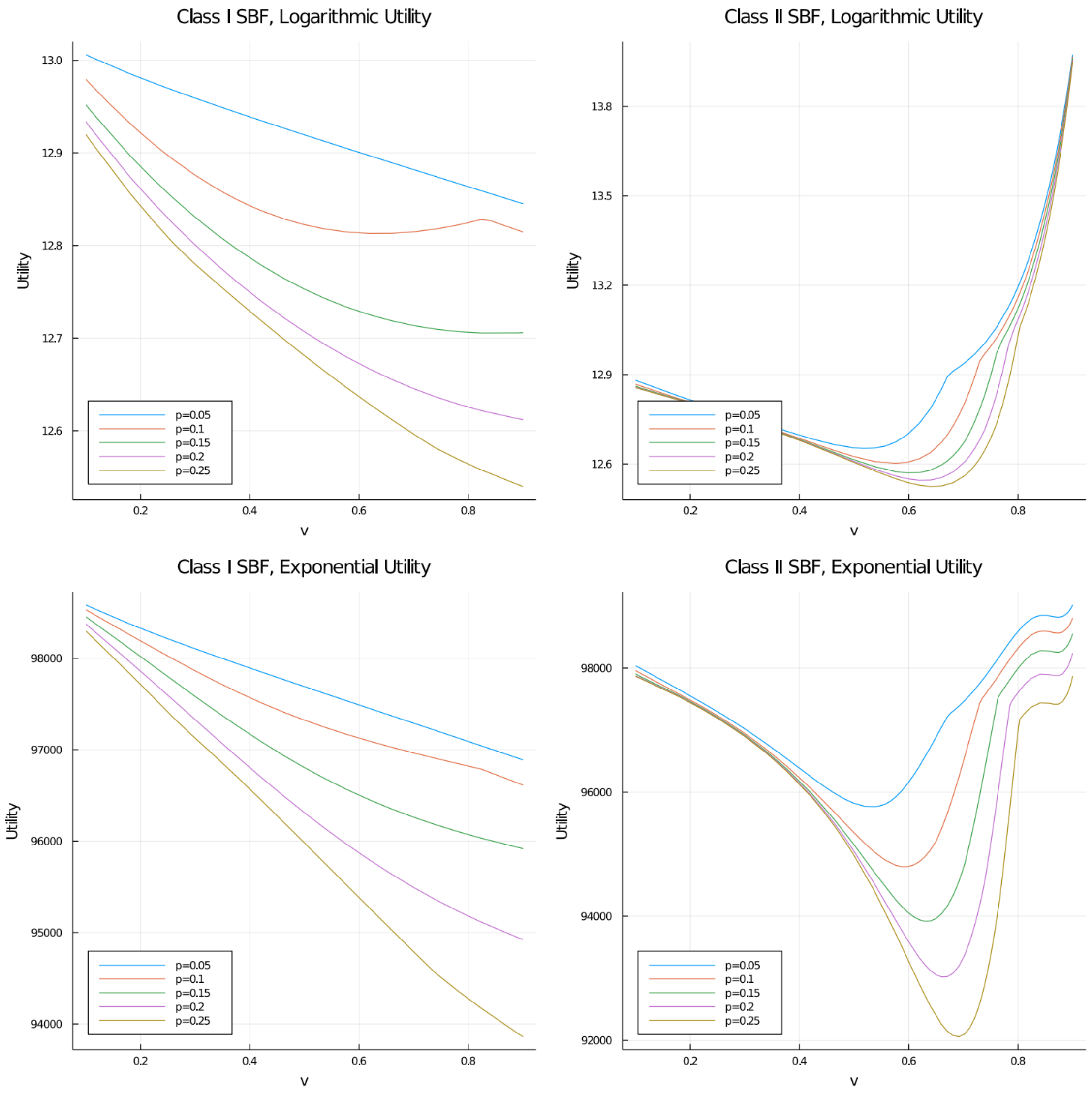
How does the model change for different vulnerabilities?



Tabular presentation of the main model results

v	$z_{max}(\$)$	$z^{I*}(\$)$	$z^{II*}(\$)$	$S^I(v, z^{I*})$	$S^{II}(v, z^{II*})$	$P^I_{max}(\$)$	$P^{II}_{max}(\$)$	$p^I_{max}(\%)$	$p^{II}_{max}(\%)$
0.20	29,430	6,363	27,264	0.183	0.104	23,067	2,166	31.6	5.2
0.25	36,788	14,983	35,207	0.204	0.120	21,805	1,581	26.7	3.3
0.30	44,146	22,776	42,826	0.224	0.138	21,369	1,320	23.9	2.4
0.35	51,503	29,943	50,203	0.242	0.159	21,561	1,300	22.3	2.0
0.40	58,861	36,613	57,336	0.258	0.182	22,248	1,525	21.5	2.1
0.45	66,218	42,878	64,140	0.274	0.209	23,340	2,079	21.3	2.5
0.50	73,576	48,803	70,413	0.289	0.240	24,773	3,163	21.5	3.3
0.55	80,933	54,439	75,772	0.303	0.279	26,494	5,162	21.9	4.6
0.60	88,291	59,824	79,506	0.316	0.326	28,467	8,785	22.5	6.7
0.65	95,649	64,989	80,292	0.329	0.387	30,659	15,357	23.3	9.9
0.70	103,006	69,959	75,541	0.342	0.467	33,047	27,465	24.2	14.7
0.75	110,364	74,755	59,829	0.354	0.579	35,609	50,534	25.2	21.8

Utility functions with varying vulnerability (optimal investment, full coverage)



Next steps…

- Multi-period case/stochastic budget?

$$B_t = B_0 - P - \sum_{t=0}^{t} (s_t^{(p)} + s_t^{(u)} - c_t)$$

- The two-state model is too simplistic; there is a rich potential avenue of research in merging rigorous analysis of systems with economic modelling.
- The choice of vulnerability parameter is pretty arbitrary; perhaps can be estimated using Partially Observable Markov Decision Processes (POMDPs)…
- Multi-attribute utility functions (e.g. combination of Confidentiality/Integrity/Availability).