

A Ruin Theory Application on Cyber Risk Modelling

Ciyu Nie (Jade)^a, Shaun Wang^a, Shuanming Li^b

^aInsurance Risk and Finance Research Centre (IRFRC)
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798

^bCentre for Actuarial Studies,
111 Barry Street, The University of Melbourne, VIC 3010, Australia

ERM Conference, September, 2016



Outline

- 1 Introduction
 - Cyber risk management
 - Classical risk process
- 2 Cyber risk model description
 - The security level process
 - The total cyber cost
- 3 Numerical examples
 - Impact of breach loss severity
 - Impact of different attack arrivals
 - Impact of time horizon
 - Impact of initial security level
- 4 Concluding Remarks



Introduction

Cyber risk model description
Numerical examples
Concluding Remarks

Cyber risk management
Classical risk process

Introduction



Literature on information system (IS) risk analysis

- Whitten & Bentley (1998): methods and frameworks to identify and manage critical risk factors in system development;
- Cohen (1997a, 1997b): extensive lists of potential attacks, defenses, threats and consequences;
- Dillon & Paté-Cornell (2008): uses a utility function to examine tradeoffs between minimization of the probability of an IS failure and maximization of the expected benefits;
- Böhme & Moore (2009): dynamic model reflecting interaction between a defender and an attacker, showed how the defender's knowledge about prospective attacks and the sunk costs incurred when upgrading defenses reactively affects the optimal security investment strategy.

In many quantitative models,

- security level is a quantifiable amount;
- security level is primarily affected by the amount of investment in security development;
- security development and the damage control scheme affect the probability and the loss severity of a defense failure.

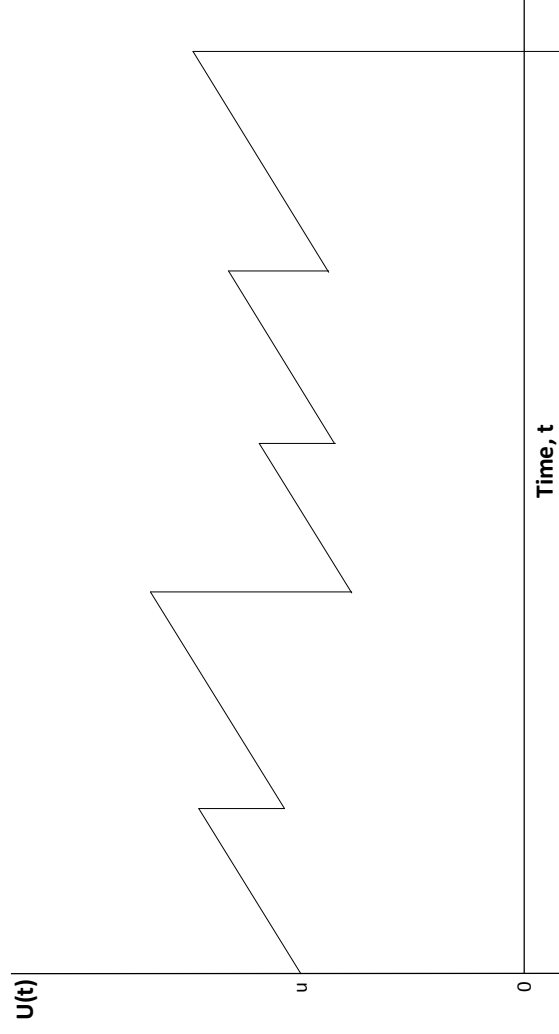
In many quantitative models,

- security level is a quantifiable amount;
- security level is primarily affected by the amount of investment in security development;
- security development and the damage control scheme affect the probability and the loss severity of a defense failure.

Challenges for cyber risk management/ cyber insurance:

- clear definition of cyber risk is still a question;
- lack of historical loss data;
- consequences of failure in defense, rather than random events;
- fast evolving nature of cyber technology.

Classical risk process:



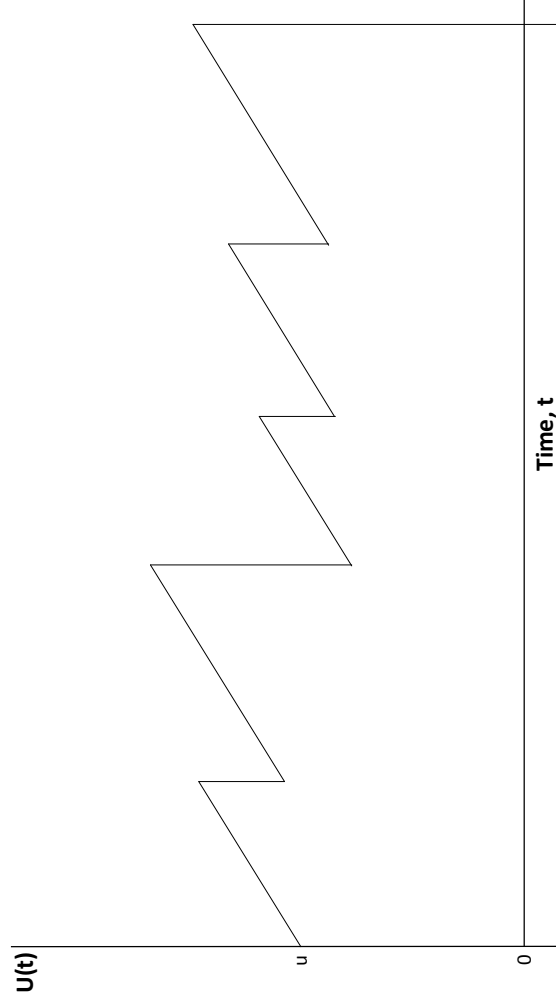
Classical risk process:

A classical risk process is defined as

$$U_t = u + ct - \sum_{i=1}^{N_t} X_i,$$

with

- u : the initial surplus level, $u \geq 0$;



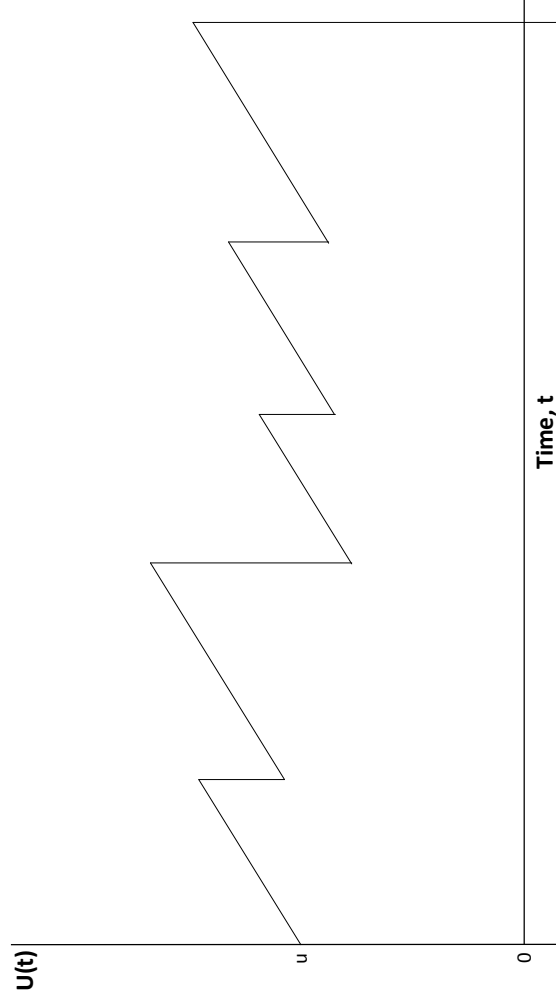
Classical risk process:

A classical risk process is defined as

$$U_t = u + ct - \sum_{i=1}^{N_t} X_i,$$

with

- u : the initial surplus level, $u \geq 0$;
- c : constant premium rate per unit time;



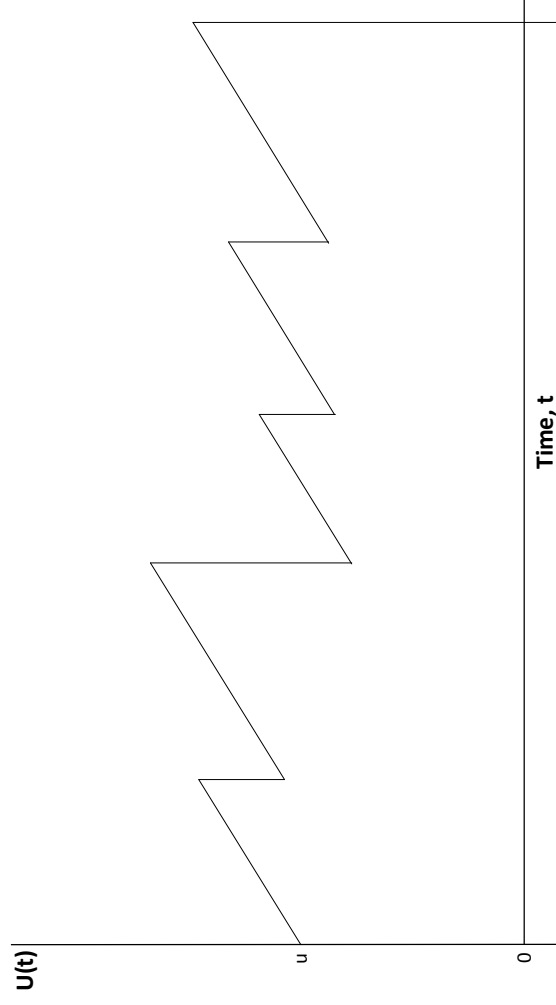
Classical risk process:

A classical risk process is defined as

$$U_t = u + ct - \sum_{i=1}^{N_t} X_i,$$

with

- u : the initial surplus level, $u \geq 0$;
- c : constant premium rate per unit time;
- $\{N_t\}_{t \geq 0}$: counting process that counts the number of claims from time 0 to t ;



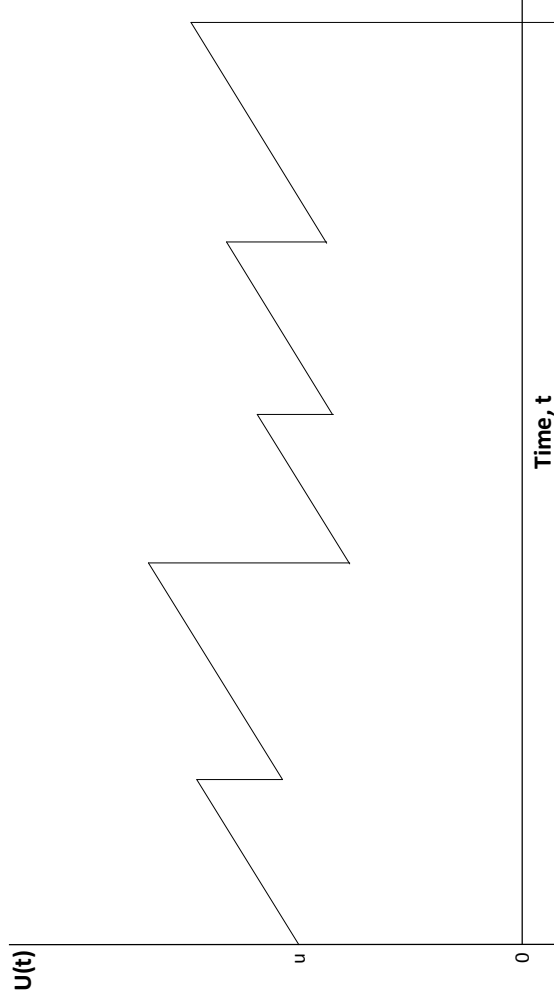
Classical risk process:

A classical risk process is defined as

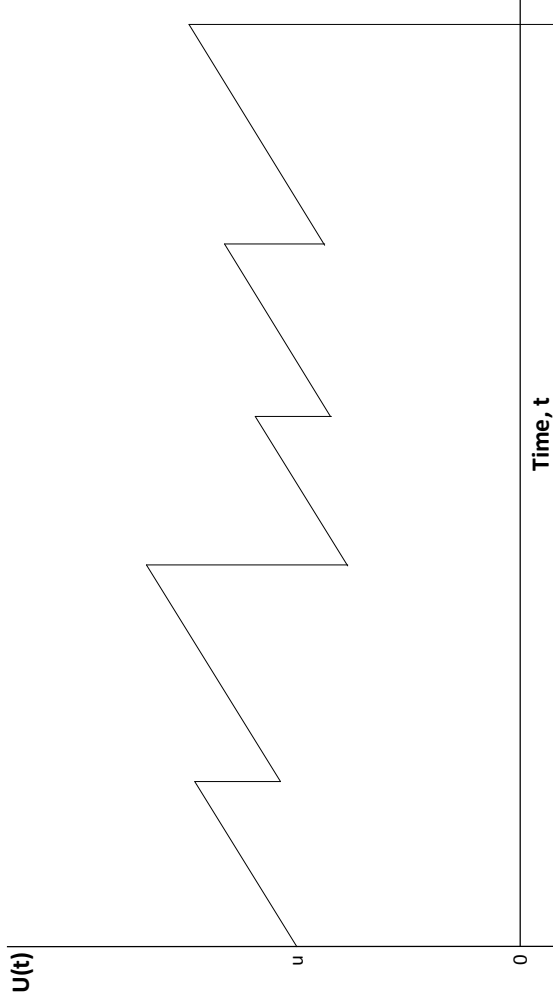
$$U_t = u + ct - \sum_{i=1}^{N_t} X_i,$$

with

- u : the initial surplus level, $u \geq 0$;
- c : constant premium rate per unit time;
- $\{N_t\}_{t \geq 0}$: counting process that counts the number of claims from time 0 to t ;
- $\{X_i\}_{i=1}^{\infty}$: the severity of claims with pdf $f(x)$, cdf $F(x)$;



Classical risk process:



A classical risk process is defined as

$$U_t = u + ct - \sum_{i=1}^{N_t} X_i,$$

with

- u : the initial surplus level, $u \geq 0$;
- c : constant premium rate per unit time;
- $\{N_t\}_{t \geq 0}$: counting process that counts the number of claims from time 0 to t ;
- $\{X_i\}_{i=1}^{\infty}$: the severity of claims with pdf $f(x)$, cdf $F(x)$;
- Ruin event: occurs when $U_t < 0$ for any $t > 0$.

Motivation

Key features of surplus process:

- assessing the dynamic change in monetary value/capital position of an insurance portfolio at any point of time;
- the process is driven by
 - an upward drift c ;
 - a downward drift caused by claims (impact determined by frequency and severity);
 - initial capital level u .

Motivation

Key features of surplus process:

- assessing the dynamic change in monetary value/capital position of an insurance portfolio at any point of time;
- the process is driven by
 - an upward drift c ;
 - a downward drift caused by claims (impact determined by frequency and severity);
 - initial capital level u .

The defense and attack forces in cyber risk management act similarly to this,

- continuous defense effort to enhance system security (such as c);
- occasional/ less continuous attack event that diminishes/compromises the established security mechanism (such as claims);
- a ruin event is similar to a failure in defense;
- initial security level has an impact on possibility of defense failure (such as u).

Motivation

Key features of surplus process:

- assessing the dynamic change in monetary value/capital position of an insurance portfolio at any point of time;
- the process is driven by
 - an upward drift c ;
 - a downward drift caused by claims (impact determined by frequency and severity);
 - initial capital level u .

The defense and attack forces in cyber risk management act similarly to this,

- continuous defense effort to enhance system security (such as c);
- occasional/ less continuous attack event that diminishes/compromises the established security mechanism (such as claims);
- a ruin event is similar to a failure in defense;
- initial security level has an impact on possibility of defense failure (such as u).



Model the defense and attack behaviour using the surplus process?



Cyber risk model description



The security level process

Assume the security level of a system is a numerical amount.



The security level process

Assume the security level of a system is a numerical amount.

The security level process: $U_t = u + ct - \sum_{i=1}^{N_t} X_i$:

- U_t : security level at any time $t \geq 0$ with $U_0 = u$;

The security level process

Assume the security level of a system is a numerical amount.

The security level process: $U_t = u + ct - \sum_{i=1}^{N_t} X_i$:

- U_t : security level at any time $t \geq 0$ with $U_0 = u$;
- ξ : amount of capital investment in security development per unit of time (a monetary term);
- $c = A(\xi)$: a continuous constant increase in security level per unit of time (referred to as security construction rate), as a result of ξ , with $A'(\xi) > 0$, $A''(\xi) \leq 0$

The security level process

Assume the security level of a system is a numerical amount.

The security level process: $U_t = u + ct - \sum_{i=1}^{N_t} X_i$:

- U_t : security level at any time $t \geq 0$ with $U_0 = u$;
- ξ : amount of capital investment in security development per unit of time (a monetary term);
- $c = A(\xi)$: a continuous constant increase in security level per unit of time (referred to as security construction rate), as a result of ξ , with $A'(\xi) > 0$, $A''(\xi) \leq 0$
- $\{N_t\}_{t \geq 0}$: number of attempted attacks during time $(0, t]$;
- $\{X_i\}_{i=1}^{\infty}$: the loss in security level caused by the i^{th} attack;

The security level process

Assume the security level of a system is a numerical amount.

The security level process: $U_t = u + ct - \sum_{i=1}^{N_t} X_i$:

- U_t : security level at any time $t \geq 0$ with $U_0 = u$;
- ξ : amount of capital investment in security development per unit of time (a monetary term);
- $c = A(\xi)$: a continuous constant increase in security level per unit of time (referred to as security construction rate), as a result of ξ , with $A'(\xi) > 0$, $A''(\xi) \leq 0$
- $\{N_t\}_{t \geq 0}$: number of attempted attacks during time $(0, t]$;
- $\{X_i\}_{i=1}^{\infty}$: the loss in security level caused by the i^{th} attack;
- A breach/defense failure: occurs when $U_t < 0$ for any $t > 0$

The security level process

Two modifications to further accommodate the modelling of cyber risks:



The security level process

Two modifications to further accommodate the modelling of cyber risks:

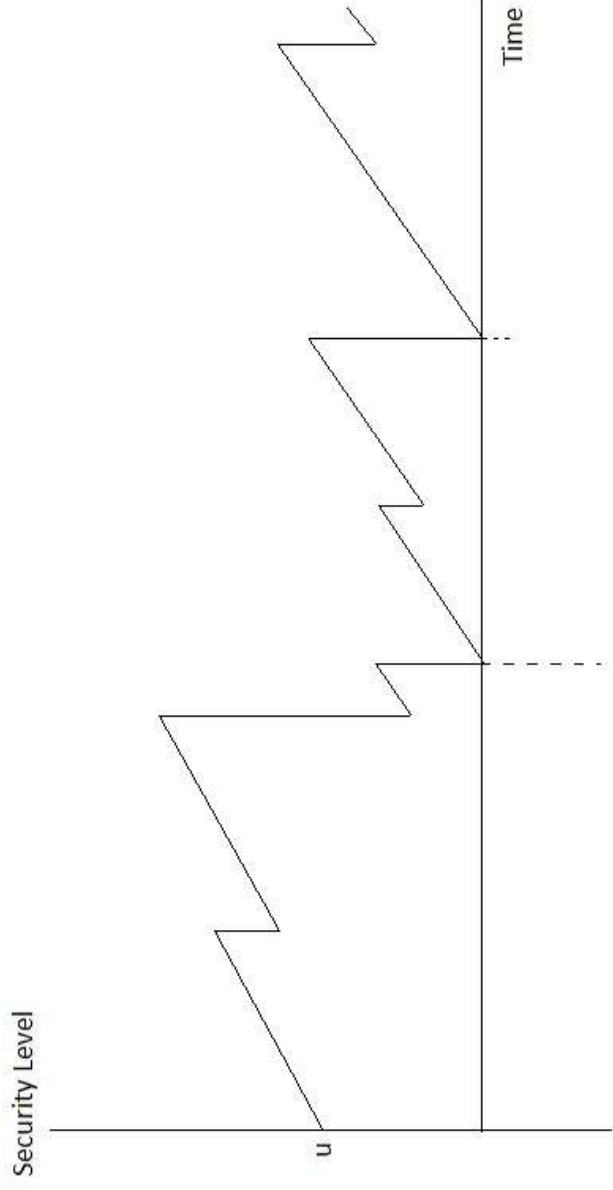
- once ruin occurs, the surplus level returns to 0 immediately and the process continues;



The security level process

Two modifications to further accommodate the modelling of cyber risks:

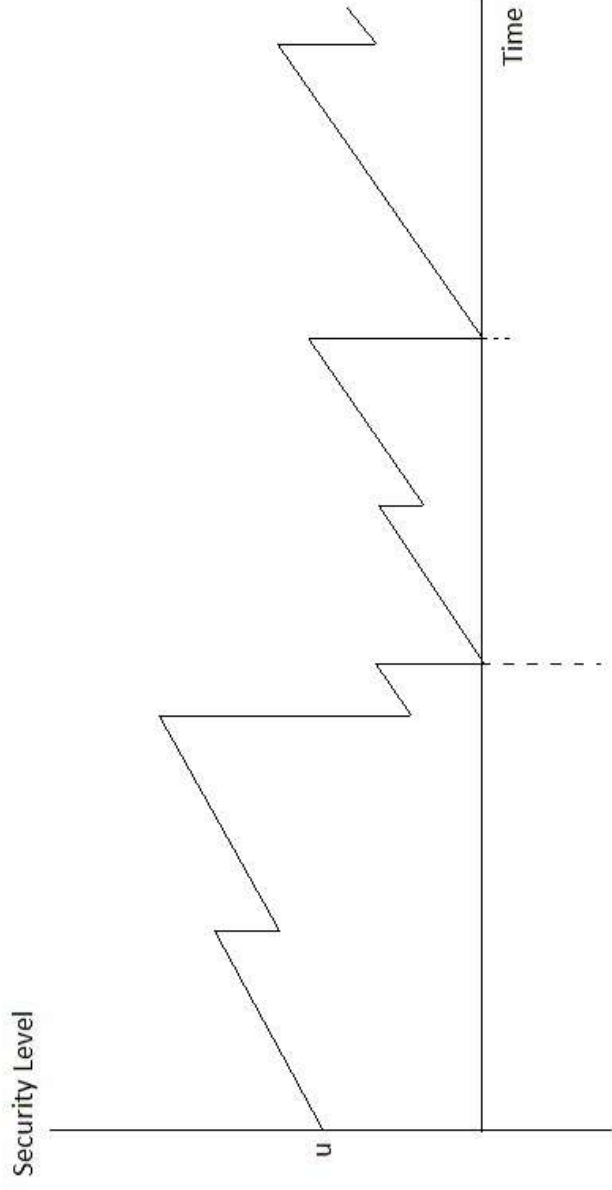
- once ruin occurs, the surplus level returns to 0 immediately and the process continues;



The security level process

Two modifications to further accommodate the modelling of cyber risks:

- once ruin occurs, the surplus level returns to 0 immediately and the process continues;
- release on the assumption for c
 - under classical ruin theory, typical to assume $c > E(N)E(X)$ to ensure $\psi(u) < 1$;
 - under cyber risk model, maybe unrealistic to assume the same for the security construction rate



The total cyber cost

Now consider

- $\{NR_u(t)\}_{t \geq 0}$: the counting process of the number of **ruin event** /security breach between time $(0, t]$, with initial surplus u , under the modified surplus process;



The total cyber cost

Now consider

- $\{NR_u(t)\}_{t \geq 0}$: the counting process of the number of **ruin event** /security breach between time $(0, t]$, with initial surplus u , under the modified surplus process;
- $\{Y_i\}_{i=1}^{\infty}$: the severity of financial loss due to a security breach;



The total cyber cost

Now consider

- $\{NR_u(t)\}_{t \geq 0}$: the counting process of the number of **ruin event** /security breach between time $(0, t]$, with initial surplus u , under the modified surplus process;
- $\{Y_i\}_{i=1}^{\infty}$: the severity of financial loss due to a security breach;

The total cyber cost between $(0, t]$ is

$$L(u, \xi, t) = \xi t + \sum_{i=1}^{NR_u(t)} Y_i,$$

and the expected total cyber costs between $(0, t]$ is

$$E[L(u, \xi, t)] = \xi t + E[NR_u(t)] * E[Y_i].$$

The total cyber cost

Now consider

- $\{NR_u(t)\}_{t \geq 0}$: the counting process of the number of **ruin event** /security breach between time $(0, t]$, with initial surplus u , under the modified surplus process;
- $\{Y_i\}_{i=1}^{\infty}$: the severity of financial loss due to a security breach;

The total cyber cost between $(0, t]$ is

$$L(u, \xi, t) = \xi t + \sum_{i=1}^{NR_u(t)} Y_i,$$

and the expected total cyber costs between $(0, t]$ is

$$E[L(u, \xi, t)] = \xi t + E[NR_u(t)] * E[Y_i].$$

Note: $L(u, \xi, t)$ represent the overall financial losses from $(0, t]$, whereas U_t represents security level at time t .



Common Notations

Notations:

- T_u : time that U_t first fall below 0 with $U_0 = u$;
- $\omega_u(t)$: defective density function of T_u ;
- $\tilde{\omega}_u(s) = \int_0^\infty e^{-st} \omega_u(t) dt, s \geq 0$: Laplace transform of $\omega_u(t)$;
- $T_{u,n}$: time of n^{th} ruin event;
- $\omega_{u,n}(t)$: defective density function of $T_{u,n}$;
- $\tilde{\omega}_{u,n}(s)$: Laplace transform of $T_{u,n}$
- $W_{u,n}(t) = \int_0^t \omega_{u,n}(\tau) d\tau$: defective cumulative distribution function of $T_{u,n}$.

General result

Probability function for $NR_u(t)$:

- For $n = 0$, $\Pr[NR_u(t) = 0] = \Pr(T_u > t) = 1 - W_u(t)$. Note that this also includes the probability that ultimate ruin never occurs.
- For $n \geq 1$,

$$\begin{aligned}\Pr[NR_u(t) = n] &= \Pr(T_{u,n} \leq t < T_{u,n+1}) \\ &= \Pr(T_{u,n} \leq t) - \Pr(T_{u,n+1} \leq t) \\ &= W_{u,n}(t) - W_{u,n+1}(t).\end{aligned}$$

- $E[NR_u(t)] = \sum_{n=1}^{\infty} n * (W_{u,n}(t) - W_{u,n+1}(t)) = \sum_{n=1}^{\infty} W_{u,n}(t)$.
- Taking the partial differentiation we have

$$\frac{\partial E[L(u, \xi, t)]}{\partial \xi} = t + E(Y_i) * A'(\xi) * \sum_{n=0}^{\infty} \frac{\partial W_{u,n}(t)}{\partial c},$$

and since $\partial W_0(t)/\partial c < 0$ and hence $\partial W_{u,n}(t)/\partial c < 0$, and that $A'(\xi) > 0$, there exists an ξ^* such that $\partial E[L(u, \xi, t)]/\partial \xi = 0$.

Numerical examples



Formulae

Given

- 1 $\{N_t\}_{t \geq 0}$: Poisson process with parameter λ ;
- 2 $\{X_i\}_{i=1}^{\infty}$ with p.d.f $f(x) = \alpha e^{-\alpha x}$,

We have

- $\tilde{\omega}_u(s) = \left(1 - \frac{R_s}{\alpha}\right) e^{-R_s u}$,

where $-R_s < 0$ is a root of the characteristic equation $x^2 + \left(\alpha - \frac{\lambda+s}{c}\right)x - \frac{\alpha s}{c} = 0$. (Geber & Shiu 1998)

- $\omega_u(t) = \sum_{j=1}^{\infty} \omega_0^{j*}(t) \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)}$, (Dickson & Li, 2010)

where $\omega_0^{j*}(t) = \frac{\lambda^j t^{j-1} e^{-(\lambda+\alpha c)t}}{\Gamma(j)} {}_0F_1(j+1; \alpha c \lambda t^2)$,

and ${}_pF_q(B_1, B_2, \dots, B_p, C_1, C_2, \dots, C_q; Z) = \sum_{m=0}^{\infty} \frac{(B_1)_m (B_2)_m \dots (B_p)_m}{(C_1)_m (C_2)_m \dots (C_q)_m} \frac{Z^m}{m!}$ is the generalised hypergeometric function and $(a)_n = \Gamma(a+n)/\Gamma(a)$ is Pochhammer's symbol. (Nie et al. 2015)

Distribution for $T_{u,n}$ in the cyber risk model:

$$\begin{aligned}\tilde{\omega}_{u,n}(s) &= \tilde{\omega}_u(s) * \tilde{\omega}_u^{\eta-1*}(s) \\ &= \sum_{j=1}^{\infty} \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)} \left(1 - \frac{R_s}{\alpha}\right)^{j+n-1}.\end{aligned}$$

$$\begin{aligned}\omega_{u,n}(t) &= \omega_u(t) * \omega_0^{\eta-1*}(t) \\ &= \sum_{j=1}^{\infty} \omega_0^{j+n-1*}(t) \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)} \\ &= \sum_{j=1}^{\infty} \frac{\lambda^{j+n-1} t^{j+n-2} e^{-(\lambda+\alpha c)t}}{\Gamma(j+n-1)} {}_0F_1(j+n; \alpha c \lambda t^2) \frac{(\alpha u)^{j-1} e^{-\alpha u}}{\Gamma(j)}.\end{aligned}$$

- We can then use numerical integration for compute $W_{u,n}(t)$.

Numerical assumptions

We focus on the value of $E[L(u, \xi, t)]$ (expected total cyber cost):

- examine the impact of various factors;
- find the optimal investment level ξ^* such that the expected cyber cost is minimized given the specific time horizon.

Numerical assumptions

We focus on the value of $E[L(u, \xi, t)]$ (expected total cyber cost):

- examine the impact of various factors;
- find the optimal investment level ξ^* such that the expected cyber cost is minimized given the specific time horizon.

Assumptions for baseline scenario:

- $u = 3$: initial security level;
- $c = A(\xi) = \ln(\xi + 1)$: security construction rate;
- $\{N_t\}_{t \geq 0}$: a Poisson process with parameter $\lambda = 1$;
- $\{X_i\}_{i=1}^{\infty}$: i.i.d. Exponential distribution with parameter $\alpha = 1$;

Numerical assumptions

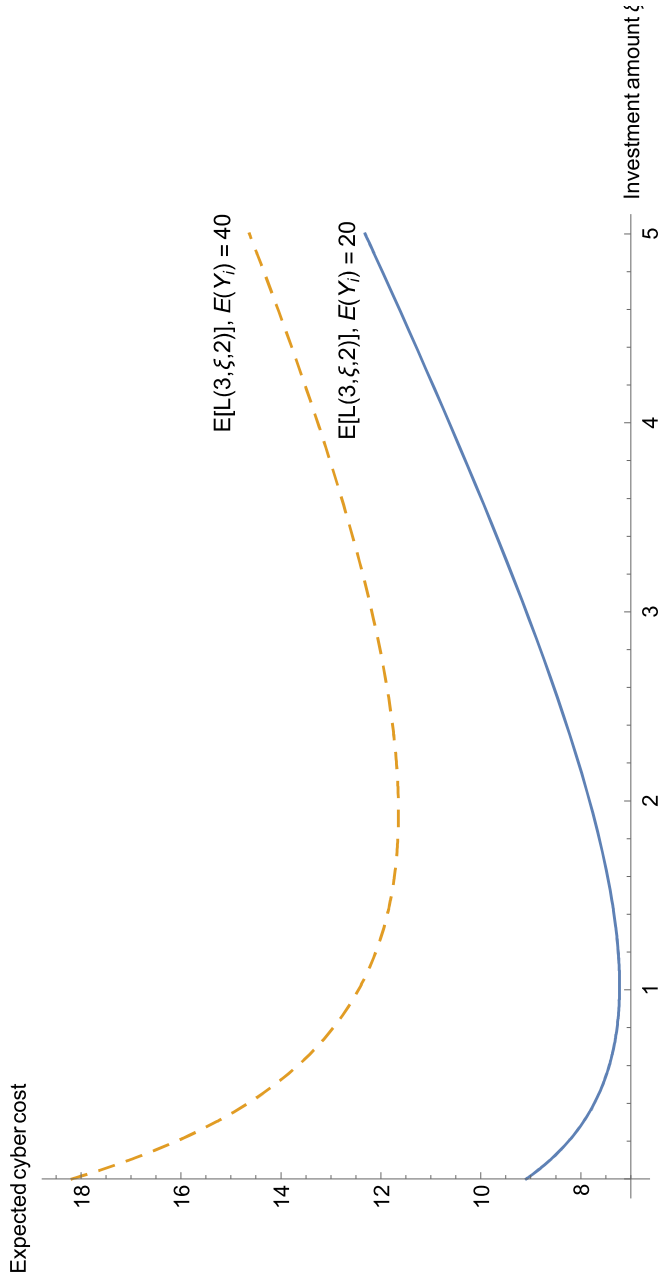
We focus on the value of $E[L(u, \xi, t)]$ (expected total cyber cost):

- examine the impact of various factors;
- find the optimal investment level ξ^* such that the expected cyber cost is minimized given the specific time horizon.

Assumptions for baseline scenario:

- $u = 3$: initial security level;
- $c = A(\xi) = \ln(\xi + 1)$: security construction rate;
- $\{N_t\}_{t \geq 0}$: a Poisson process with parameter $\lambda = 1$;
- $\{X_i\}_{i=1}^{\infty}$: i.i.d. Exponential distribution with parameter $\alpha = 1$;
- $t = 2$: time horizon is 2 units of time;
- $E(Y_i) = 20$: the expected financial loss upon defense failure.

Figure: Expected number of breach with different $E(Y_i)$



Optimal investment level:

- When $E(Y_i) = 20$, $\xi^* = 1.0231$, $E[L(3, 1.0231, 2)]^* = 7.2240$.
Note that with $\xi^* = 1.0231$, $c = 0.7046 < \lambda/\alpha$;
- When $E(Y_i) = 40$, $\xi^* = 1.9377$, $E[L(3, 1.9377, 2)]^* = 11.6481$;

Figure: Expected number of breach with different attack arrivals

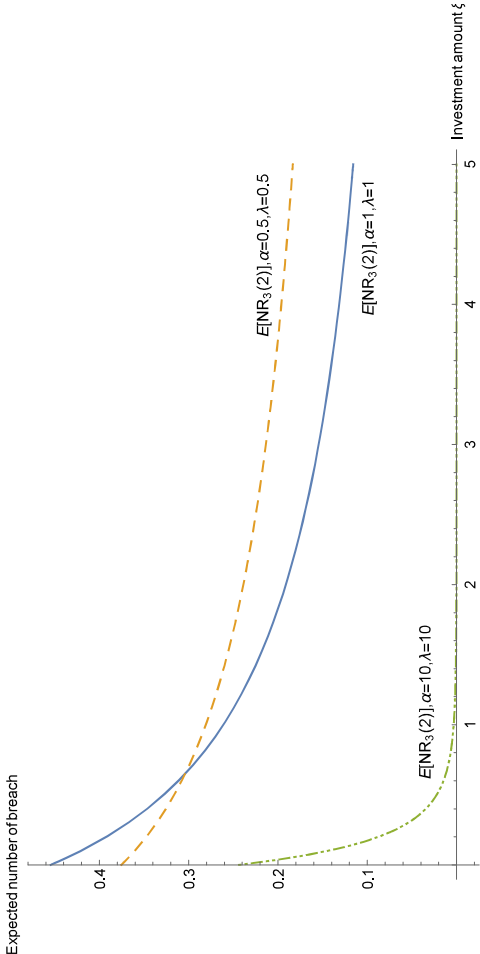


Figure: Total expected cyber cost with different attack arrivals

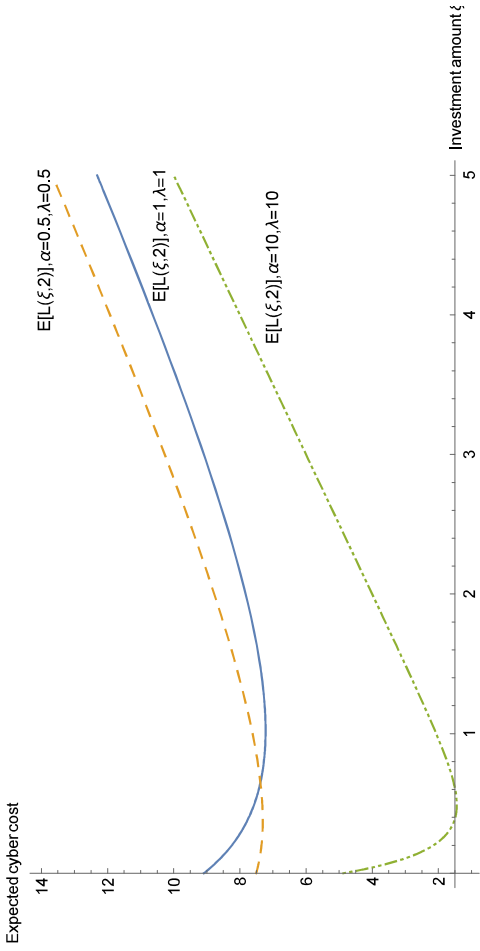
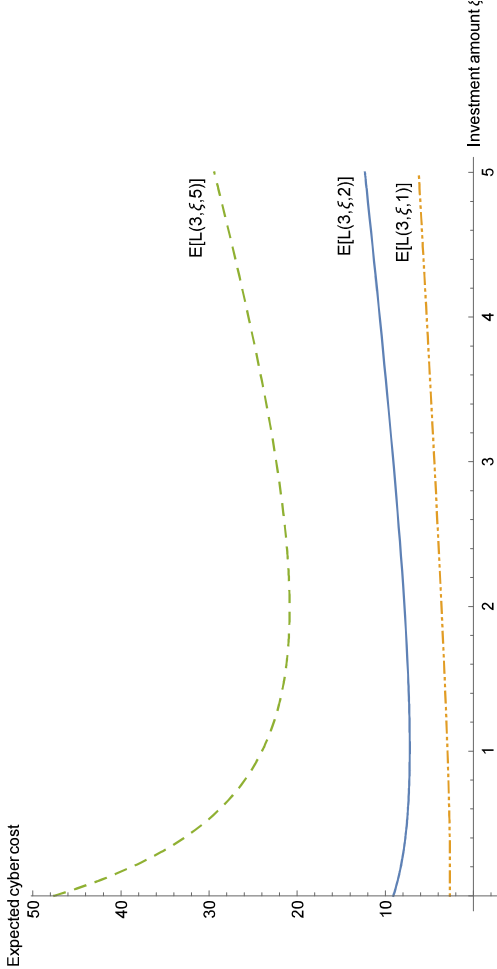


Table: Optimal ξ with different attack arrivals

Parameters	$E(L)^*$	ξ^*	$E[NR_3(t)]^*$
$\lambda = 1, \alpha = 1$	7.2240	1.0231	0.2589
$\lambda = 0.5, \alpha = 0.5$	7.3091	0.3757	0.3279
$\lambda = 10, \alpha = 10$	1.4452	0.4890	0.02336

Figure: Total expected cyber cost with different t

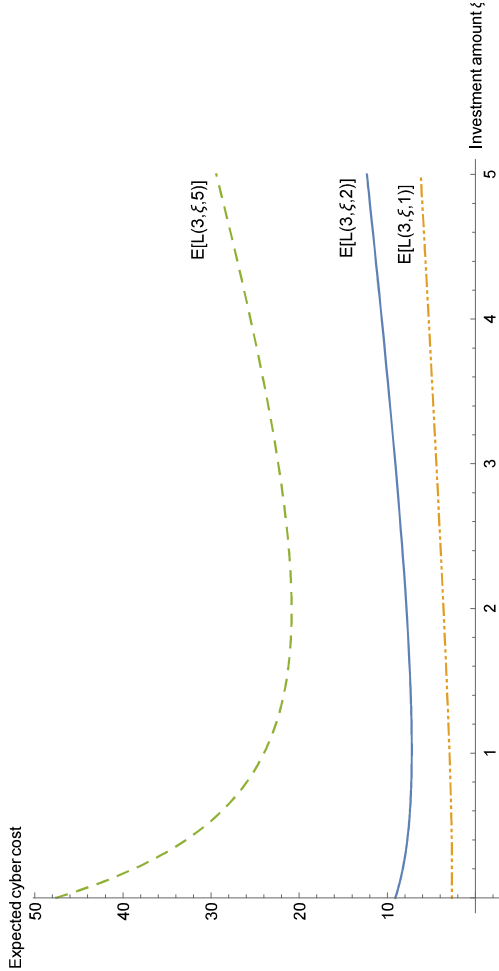


- As t increases, the expected total cyber cost shifts upward;

Table: Optimal ξ with different t

Time	$E(L)^*$	ξ^*	$E[NR_u(t)]^*$	$E[NR_u(t)]^*/t$
$t = 1$	2.6584	0.1688	0.1245	0.1245
$t = 2$	7.2240	1.0231	0.2589	0.1294
$t = 5$	20.8592	1.9877	0.5460	0.1092

Figure: Total expected cyber cost with different t



- As t increases, the expected total cyber cost shifts upward;
- For longer time horizon, optimal to invest more in security development;

Table: Optimal ξ with different t

Time	$E(L)^*$	ξ^*	$E[NR_u(t)]^*$	$E[NR_u(t)]^*/t$
$t = 1$	2.6584	0.1688	0.1245	0.1245
$t = 2$	7.2240	1.0231	0.2589	0.1294
$t = 5$	20.8592	1.9877	0.5460	0.1092

Figure: Total expected cyber cost with different t

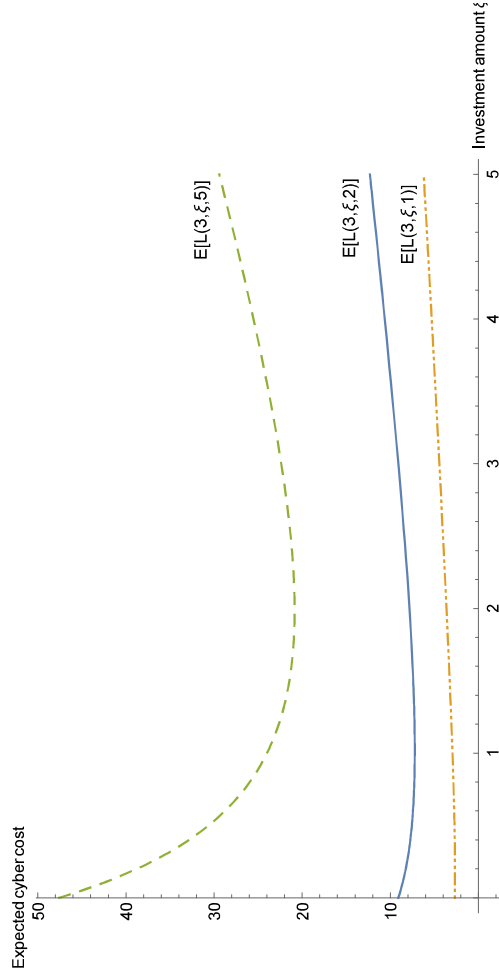


Table: Optimal ξ with different t

Time	$E(L)^*$	ξ^*	$E[NR_u(t)]^*$	$E[NR_u(t)]^* / t$
$t = 1$	2.6584	0.1688	0.1245	0.1245
$t = 2$	7.2240	1.0231	0.2589	0.1294
$t = 5$	20.8592	1.9877	0.5460	0.1092

- As t increases, the expected total cyber cost shifts upward;
- For longer time horizon, optimal to invest more in security development;
- $E(L)^*$ not linearly related to t
 - at the end of one time unit, the security level may be lower or higher than the start of the year
 - optimal level of investment will change accordingly for the next year

Figure: Total expected cyber cost with different t

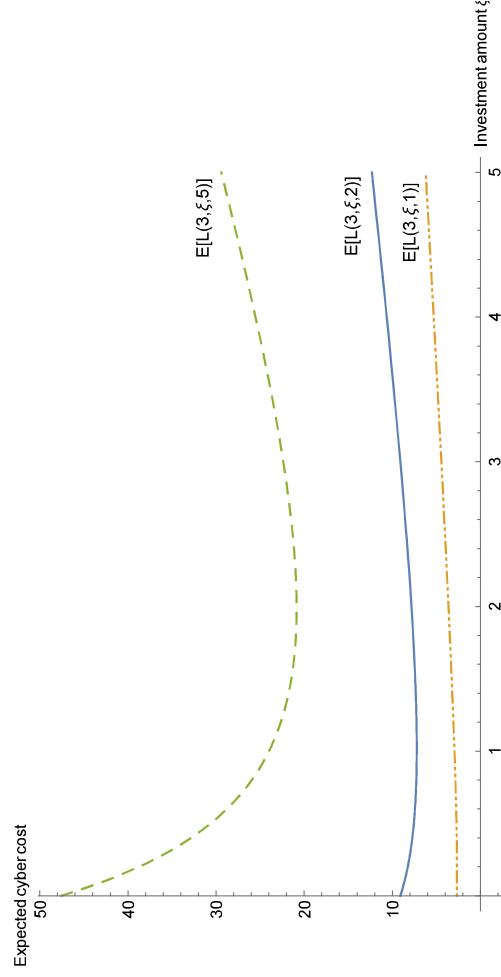


Table: Optimal ξ with different t

Time	$E(L)^*$	ξ^*	$E[NR_u(t)]^*$	$E[NR_u(t)]^*/t$
$t = 1$	2.6584	0.1688	0.1245	0.1245
$t = 2$	7.2240	1.0231	0.2589	0.1294
$t = 5$	20.8592	1.9877	0.5460	0.1092

- As t increases, the expected total cyber cost shifts upward;
- For longer time horizon, optimal to invest more in security development;
- $E(L)^*$ not linearly related to t
 - at the end of one time unit, the security level may be lower or higher than the start of the year
 - optimal level of investment will change accordingly for the next year
- Selection of time horizon is important when planning for cyber risk management.

Figure: Total expected cyber cost with different u

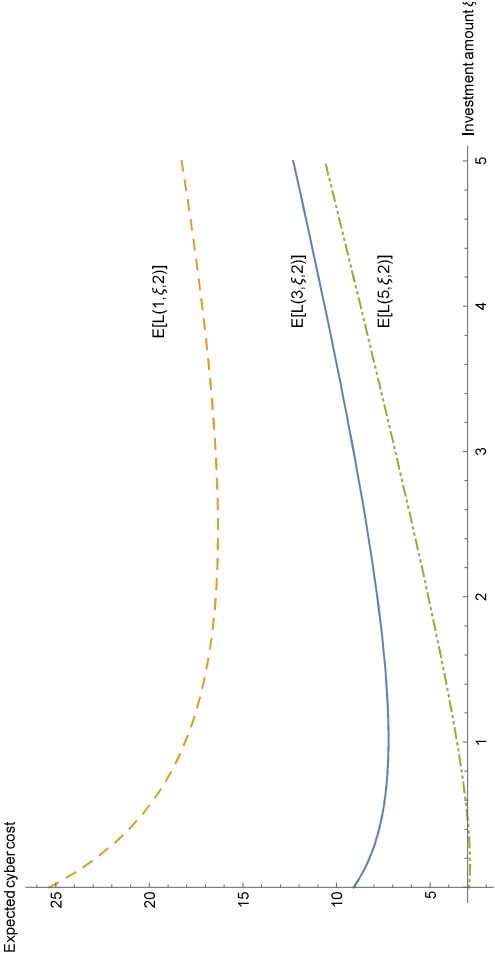
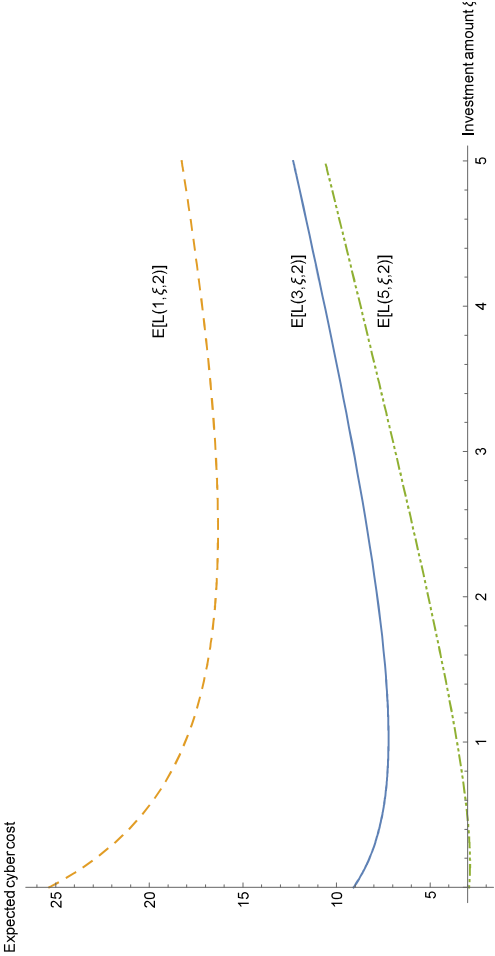


Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615



Figure: Total expected cyber cost with different u



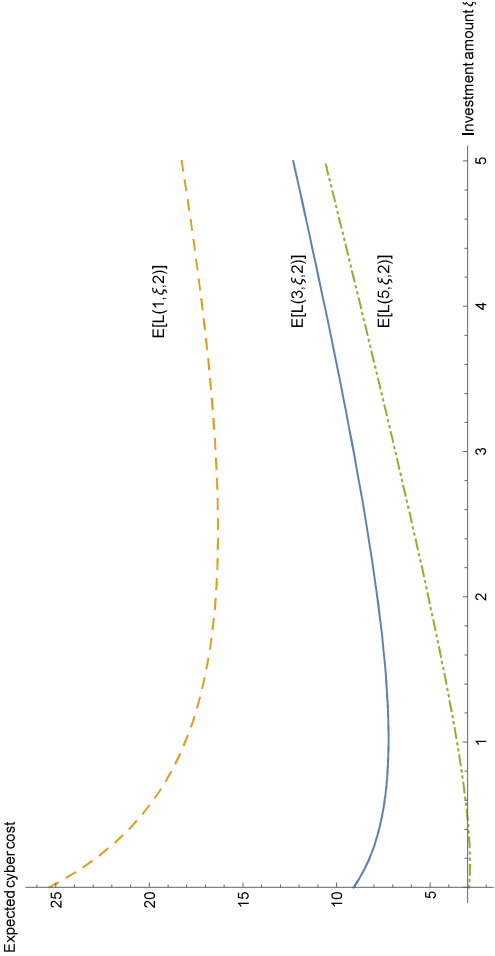
Assume we can invest ξ_a^b , $a < b$, to instantly increase U_t from a to b . We also assume that $\xi_a^b \geq A^{-1}(b - a)$

- if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time.

Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615

Figure: Total expected cyber cost with different u



Assume we can invest ξ_a^b , $a < b$, to instantly increase U_t from a to b . We also assume that $\xi_a^b \geq A^{-1}(b - a)$

- if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time.

If at time $t = 0$ and $u = a$, expected total cyber cost: $E[L(a, \xi, t)]$.

Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615

Figure: Total expected cyber cost with different u

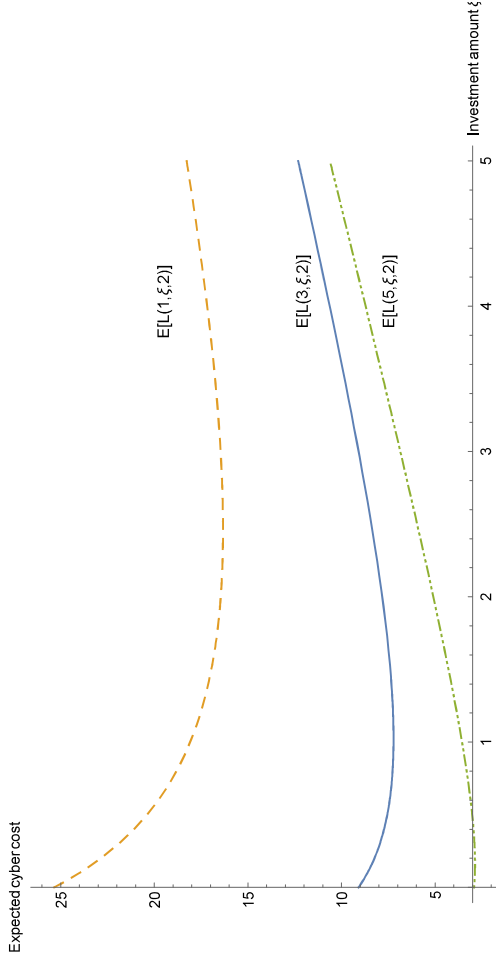


Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615

Assume we can invest ξ_a^b , $a < b$, to instantly increase U_t from a to b . We also assume that $\xi_a^b \geq A^{-1}(b - a)$

- if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time.

If at time $t = 0$ and $u = a$, expected total cyber cost: $E[L(a, \xi, t)]$.

We decide to invest ξ_a^b such that the initial u increases to b instantly, expected total cyber cost is then $\xi_a^b + E[L(b, \xi, t)]$.

Figure: Total expected cyber cost with different u

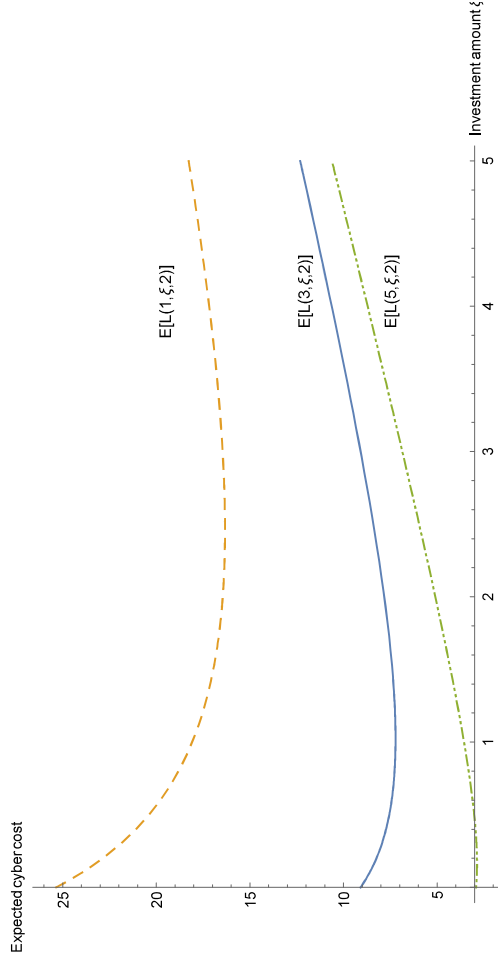


Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615

Assume we can invest ξ_a^b , $a < b$, to instantly increase U_t from a to b . We also assume that $\xi_a^b \geq A^{-1}(b - a)$

- if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time.

If at time $t = 0$ and $u = a$, expected total cyber cost: $E[L(a, \xi, t)]$.

We decide to invest ξ_a^b such that the initial u increases to b instantly, expected total cyber cost is then $\xi_a^b + E[L(b, \xi, t)]$.

Given $c = \ln(\xi + 1)$, we have $\xi_1^3 \geq 6.3891$.

Figure: Total expected cyber cost with different u

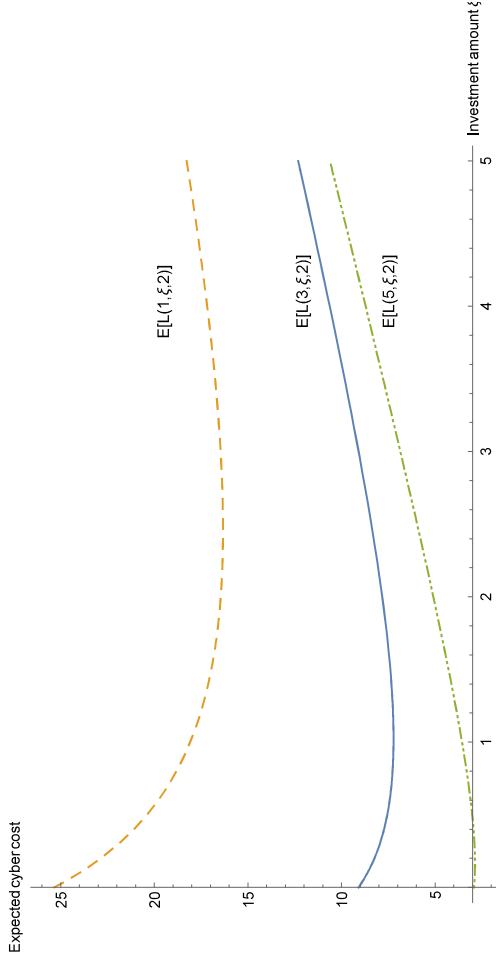


Table: Optimal ξ with different u

Initial u	$E(L)^*$	ξ^*
$u = 1$	16.3325	2.4618
$u = 3$	7.2240	1.0231
$u = 5$	2.8710	0.1615



Assume we can invest ξ_a^b , $a < b$, to instantly increase U_t from a to b . We also assume that $\xi_a^b \geq A^{-1}(b - a)$

- if we want to increase U_t from a to b instantly, it will cost more than develop U_t from a to b during 1 unit time.

If at time $t = 0$ and $u = a$, expected total cyber cost: $E[L(a, \xi, t)]$.

We decide to invest ξ_a^b such that the initial u increases to b instantly, expected total cyber cost is then $\xi_a^b + E[L(b, \xi, t)]$.

Given $c = \ln(\xi + 1)$, we have $\xi_1^3 \geq 6.3891$.

If $\xi_1^3 \leq 9.1085$, we can reduce the total expected cyber cost by a one-off investment to boost the initial security level from 1 to 3.

Remark

- We apply a ruin theory framework on cyber risk modelling and it is to our knowledge the first attempt to do so in ruin theory literature;
- Instead of direct estimation of cyber loss frequency, we used a surplus process to model the defense and attack behaviour of the information system, and hence generated the cyber loss frequency by counting the ruin events.
- Unlike traditional ruin theory studies that mostly focused on ultimate ruin probabilities, we relaxed the constraint on “premium income” and therefore focused on finite time ruin scenarios.



References

-  Böhme, R. and Moore, T. (2009).
“The iterated weakest link: A model of adaptive security investment”.
WEIS: 8th Workshop on the Economics of Information Security, June 24&25 , London,
UK.
-  Cohen, F. (1997a)
“Information system attacks: a preliminary classification scheme”.
Computers & Security, 16: 29-46.
-  Cohen, F. (1997b)
“Information system defences: a preliminary classification scheme”.
Computers & Security, 16: 94-114.
-  Dickson, D.C.M. (2005).
Insurance Risk and Ruin. Cambridge University Press, Cambridge.



References



Dickson, D.C.M. and Li, S. (2010).
“Finite time ruin problems for the Erlang(2) risk model”.
Insurance: Mathematics and Economics, 46: 12-18.



Dillon, R. L. & Paté-Cornell, M. E. (2008)
“Including Technical and Security Risks in the Development of Information Systems: A
Programmatic Risk Management Model”.
Systems Engineering, 8(1): 15-28.



Gerber, H.U. and Shiu, E.S.W. (1998)
“On the Time Value of Ruin”.
North American Actuarial Journal, 2: 48-78.



Nie, C., David, D.C.M and Li, S. (2015).
“The finite time ruin probability in a risk model with capital injections”.
Scandinavian Actuarial Journal, 4: 301-318.



Whitten, J.L. and Bentley, L.D. (1998)
Systems Analysis and Design Methods, 4th edition. Irwin McGraww-Hill.



Q & A

- 1 Introduction
 - Cyber risk management
 - Classical risk process
- 2 Cyber risk model description
 - The security level process
 - The total cyber cost
- 3 Numerical examples
 - Impact of breach loss severity
 - Impact of different attack arrivals
 - Impact of time horizon
 - Impact of initial security level
- 4 Concluding Remarks



Thank You!

