Cyber Risk Quantification: Risk Dependency and Its Impact on Modeling and Underwriting

Mingyan Liu

Peter & Evelyn Fuss Chair of Electrical and Computer Engineering
Professor of Electrical Engineering & Computer Science

University of Michigan, Ann Arbor

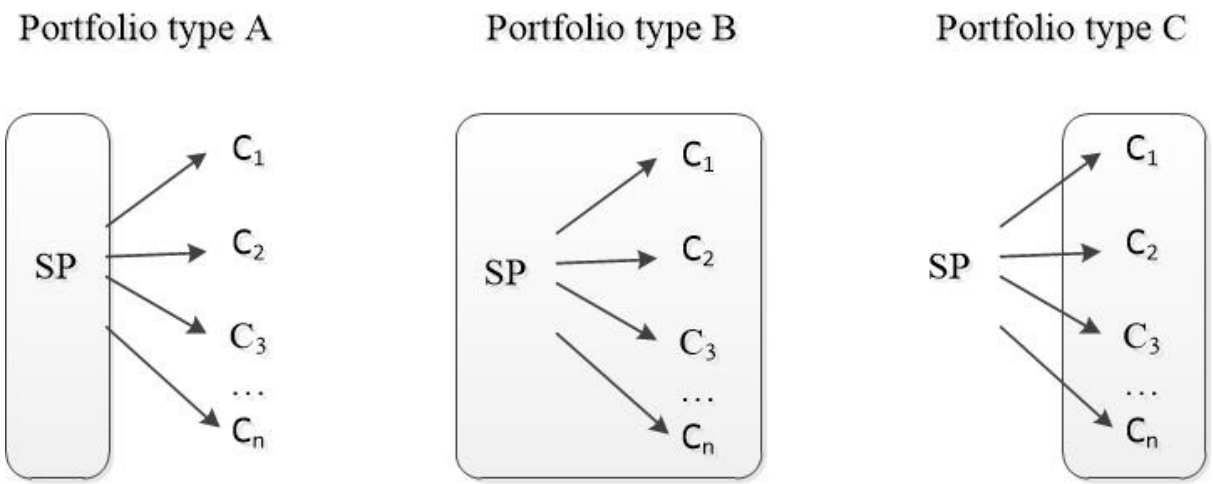
Motivation: a story of interdependent risk

- Firms increasingly turning to cyber insurance to help manage losses from cyber incidents.
  - U.S. premiums expected to exceed $14B in just a few years.
- Carriers scrambling to understand and manage cyber risks, including their own.
  - One key concern: systemic risk (aggregated, or correlated, risk), stemming from interdependent IT systems among policy holders.
- Example: a service provider (SP) with many customers:
  - Cloud, network infrastructure, application hosting, etc.
  - Each customer's operation depends not only its own actions but that of the SP's; e.g., incident to the latter can cause business interruption/losses to the former.

Research question & overview

How to take risk dependency into account when designing policies?

- Consider three portfolio types:



- Use contract theory to understand the difference in the carrier's profit and in the overall security level:
  - we will rely on an actual cyber-insurance policy rate schedule;
  - we will also use insurance claims data.

Underwriting using a rate schedule

Base premium and base retention for $1M in coverage (financial firms):

Asset Size	Base Premium	Base Retention
$0 to $ 100,000,000	$5,000	$25,000
$100,000,001 to $250,000,000	$7,000	$25,000
$250,000,001 to $500,000,000	$8,500	$50,000
$500,000,001 to $1,000,000,000	$11,000	$100,000
⋮	⋮	⋮

Underwriting using a rate schedule

Base premium and base retention \$1M in coverage (non-financial firms):

Annual Revenue	Base Premium	Base Retention
\$0 to \$5,000,000	\$5,000	\$25,000
\$5,000,001 to \$10,000,000	\$7,500	\$25,000
\$10,000,001 to \$25,000,000	\$11,500	\$25,000
\$25,000,001 to \$50,000,000	\$16,500	\$50,000
⋮	⋮	⋮

Underwriting using a rate schedule

The base rate is then multiplied by a number of factors:

- Industry Factor

Industry	Factor
Agriculture	0.85
Construction	0.85
Not-for-Profit Organizations	1.00
Technology Service Providers	1.2
Telecommunications	1.2

Underwriting using a rate schedule

The base rate is then multiplied by a number of factors:

- Industry Factor
- Retention Factor

Selected Retention	Base Retention			
	$25,000	$100,000	$500,000	$1000,000
$25,000	**1.00**	1.16	1.34	1.47
$100,000	0.87	**1.00**	1.16	1.27
$500,000	0.75	0.87	**1.00**	1.10
$1,000,000	0.68	0.79	0.91	**1.00**

Underwriting using a rate schedule

The base rate is then multiplied by a number of factors:

- Industry Factor
- Retention Factor
- Increased limit factor

Coverage Limit	Increased Limit Factor
\$1,000,000	1.000
\$2,500,000	1.865
\$5,000,000	2.987
\$10,000,000	4.786
\$25,000,000	8.925

Underwriting using a rate schedule

The base rate is then multiplied by a number of factors:

- Industry Factor
- Retention Factor
- Increased limit factor
- Co-insurance factor

Co-Insurance %	Co-insurance Factor
0%	1.000
1.0%	0.995
5.0%	0.980
10%	0.960
20%	0.920
50%	0.780

Underwriting using a rate schedule

The base rate is then multiplied by a number of factors:

- Industry Factor
- Retention Factor
- Increased limit factor
- Co-insurance factor
- First/Third-party modifier factors (Cybersecurity factors)
- Optional coverage grants such as privacy costs or crisis management.

An example

A non-financial Technology Service Provider with annual revenue \$6M purchasing a policy with retention \$100,000 and coverage limit \$2.5M.

- Base premium: \$7,500; Base retention: \$25,000 (for \$1M limit)
- Industry factor: 1.2.
- Retention factor: 0.87.
- Limit factor: 1.865.
- First/Third-party modifier factor: 1.
- Co-insurance factor: 1.
- Privacy notification: 0.15 (for base premium/retention)
- Crisis management: 0.02 (for base premium/retention)

Total premium:
$(7500)(1.2)(0.87)(1.865)(1)(1) + (7500)(0.15 + 0.02) = \$15,877.95$

First-party modifier factor

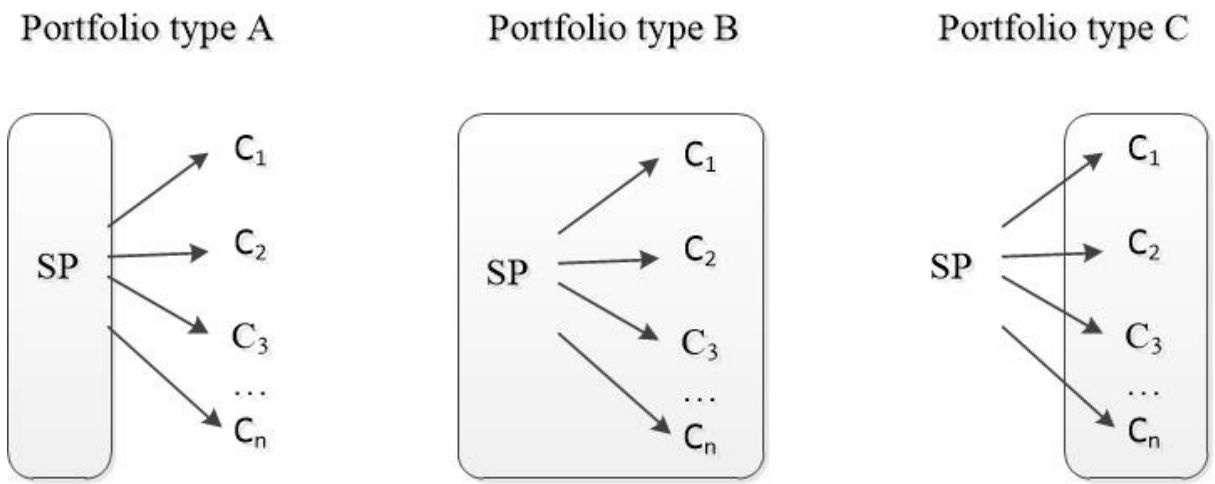
- InfoSec security policy
  - Does the insured maintain an information systems security policy?
  - Is it kept current/reviewed at least annually/updated as necessary?
  - YES to 2 of the above (0.8-0.9), 1 (0.95-1.05), 0 (1.1-1.2).
- Laptop security policy
  - Does the insured have a laptop security policy?
  - Yes (0.8-0.9), N/A (1), No (1.1-1.2)
- Web server security
  - Is sensitive data stored on web servers?
  - No (0.9-1), Yes (1.1-1.2)
- Disaster recovery
  - Does the insured have a computer disaster recovery plan?
  - Is it reviewed and updated at least bi-annually?
  - Is it tested at least annually?
  - YES to 3 (0.8-0.9), 2 (0.91-0.99), 3 (1-1.05), 0 (1.06-1.15).

Third-party modifier factor

- Website third-party service provider
  - Is a written agreement in place between the insured and the provider?
  - Does the agreement require a level of security commensurate with the insureds information systems security policy?
  - Does the insured review the results of the most recent SAS 70 or commensurate risk assessment?
  - YES to N/A (1), 3 (0.8-0.9), 2 (0.91-0.99), 3 (1-1.05), 4 (1.06-1.15)
- Application service provider
- Infrastructure operations third-party provider
- Backup & archiving third-party provider

Main observation and ideas

- The third-party modifier factor is not actually third-party risk specific, and it should be.



  - It can be estimated externally for Portfolio C.
  - It is available to the underwriter for Portfolios A (becomes first-party) and B.
- The analysis will now proceed by ignoring all other factors.

The model: Portfolio A

Service provider (SP):

- Base Premium b_o
- Retention d_o
- Cyber risk factor f_o
- *Incentive factor* f_o'
- Pays $b_o \cdot (f_o - f_o')$ as premium.
- Gets coverage $L_o - d_o$ upon an incident with loss amount L_o.
- SP's probability of suffering a loss is $P_o(f_o - f_o')$ where $P_o(.)$ is an increasing and convex function.

Insurer's expected profit as function of f_o':

$$\overline{V}_o(f_o') = b_o \cdot (f_o - f_o') - P_o(f_o - f_o') \cdot \underbrace{E\{(L_o - d_o)^+\}}_{l_o}$$

The model: Portfolio B

SP's customer i:

- Base premium b_i
- Retention d_i
- Cyber risk factor f_i, uniformly distributed in $[f_{min}, f_{max}]$.
- Pays $b_i \cdot f_i$ in premium.
- Gets coverage $L_i - d_i$ upon an incident with loss amount L_i.
- If an incident happens to SP, with probability t it affects i.
- An incident can occur to i *not* due to SP with probability $P_i(f_i)$.
- The total probability of a loss incident for i:

$$P_{li}(f_o', f_i) = P_i(f_i) + t \cdot P_o(f_o - f_o') \cdot (1 - P_i(f_i))$$

Insurer's profit from i as function of f_o':

$$\overline{V}_i(f_o') = b_i \frac{f_{min} + f_{max}}{2} - E_{f_i}[P_{li}(f_o', f_i)] \cdot l_i$$

The model: Portfolio C

Portfolio Type C: insure only customers; recover loss from the SP's policy.

- Third-party (SP) insurer profit:

$$\begin{aligned}\overline{U}_o(f_o') &= b_o \cdot (f_o - f_o') - P_o(f_o - f_o') \cdot l_o \\ &- \sum_i q \cdot [t \cdot P_o(f_o - f_o')] \cdot [1 - P_i(f_i)] \cdot l_i\end{aligned}$$

  - q: the probability of attributing the loss to the SP.

- Primary party (i) insurer profit:

$$\overline{U}_i(f_o') = b_i \cdot f_i - \{P_i(f_i) + (1-q) \cdot [t \cdot P_o(f_o - f_o')] \cdot [1 - P_i(f_i)]\} \cdot l_i$$

The model: comparison

- Portfolio A

$$f_o^* = \arg\max_{f_o'} \overline{V}_o(f_o')$$

- Portfolio B

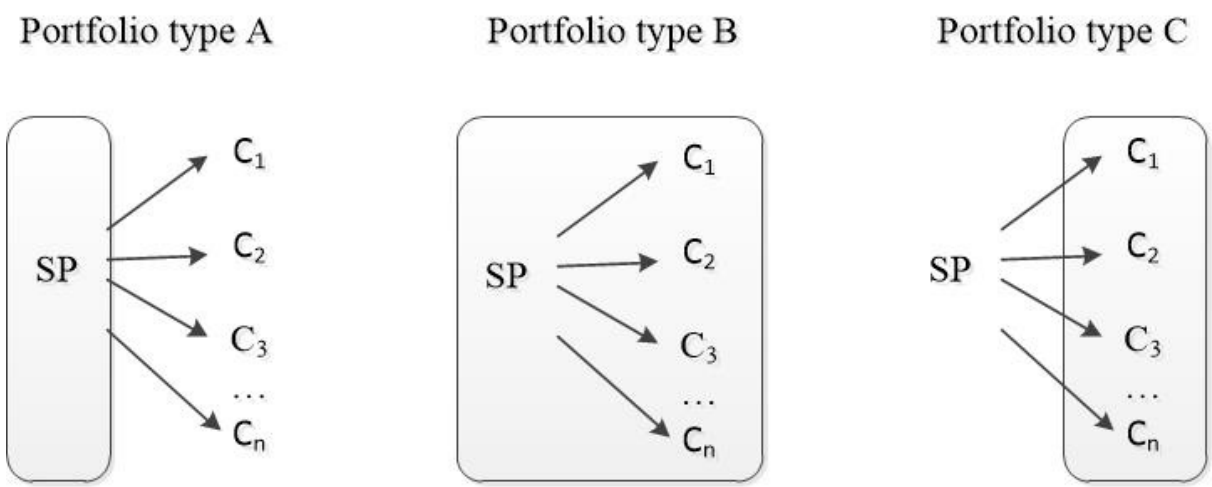
$$f_o^{**} = \arg\max_{f_o'} \overline{V}_o(f_o') + \sum_i \overline{V}_i(f_o')$$

- Portfolio C

$$f_o^{***} = \arg\max_{f_o'} \overline{U}_o(f_o')$$

Main Results

- $f^{**} \geq f^{***} \geq f^{*}$ – the insurer offers higher incentive to reduce the SP's risk when it insures both the SP and its customers.
- The incentive, f^{**}, is increasing in n, the number of SP's customers.
- The profit maximizing strategy is to insure *both* the SP and its customers (Portfolio B): $\overline{V}_o(f^{**}) + \sum_i \overline{V}_i(f^{**}) \geq \sum_i \overline{U}_i(f^{***})$
- Portfolio B is also yields the highest social welfare among the three.



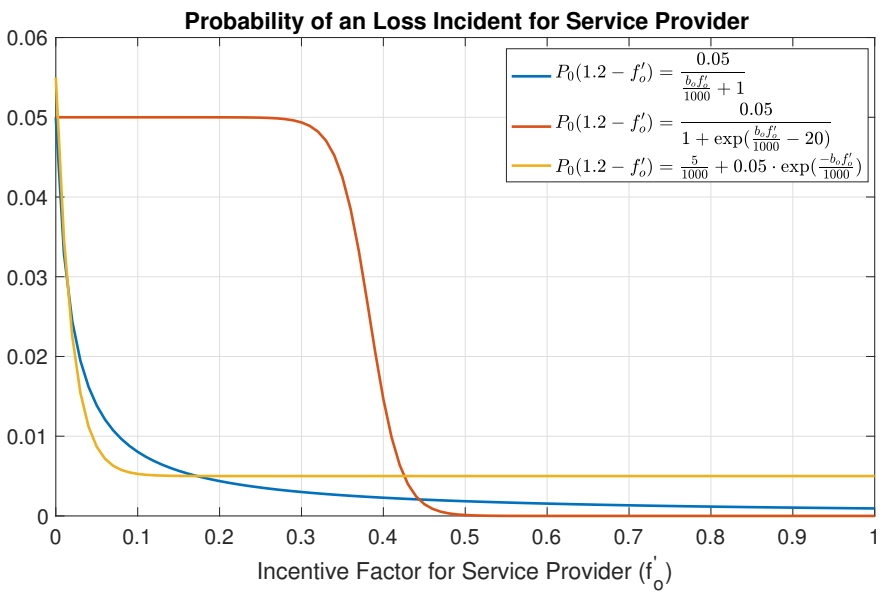
Loss Probability Functions

Intention is to capture different types of shapes

$$P_o(f_o - f_o') = \frac{0.05}{\frac{b_o(1.2-(f_o-f_o'))}{1000} + 1} \text{ (blue)} \quad (1)$$

$$P_o(f_o - f_o') = \frac{0.05}{(1 + \exp(\frac{b_o \cdot (1.2-(f_o-f_o'))}{1000} - 20))} \text{ (red)} \quad (2)$$

$$P_o(f_o - f_o') = \frac{5}{1000} + 0.05 \cdot \exp(-\frac{b_o \cdot (1.2 - (f_o - f_o'))}{1000}) \text{ (yellow)} \quad (3)$$

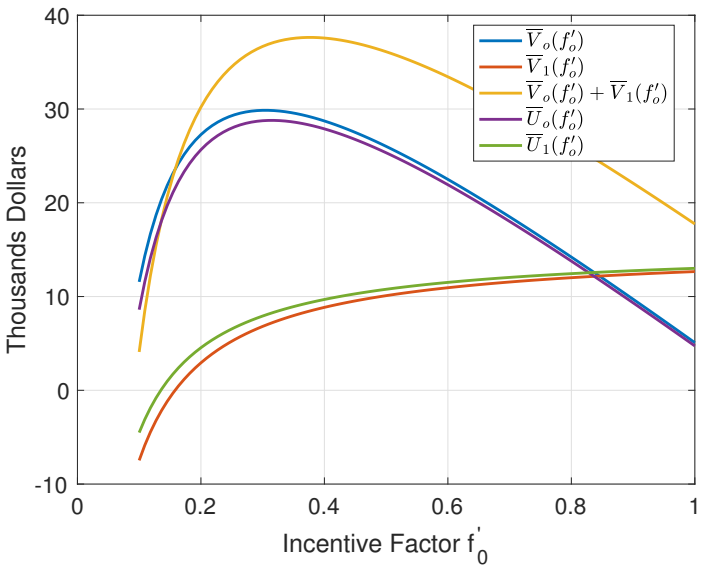


Numerical Example

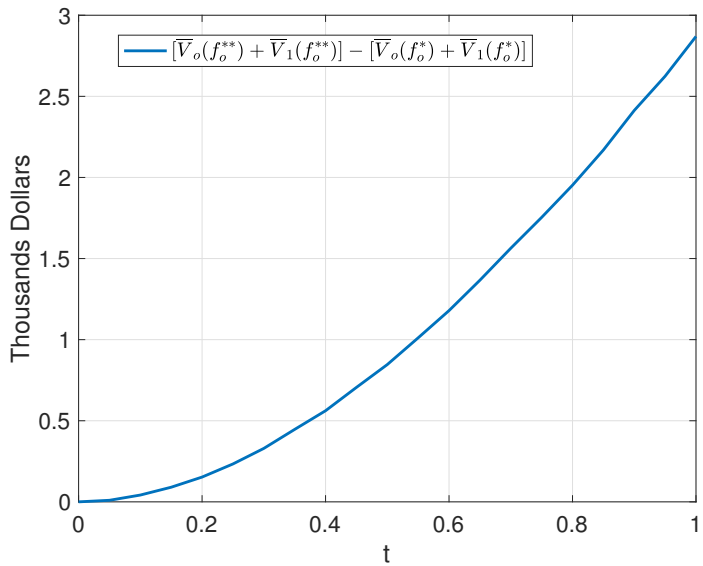
- An SP and a single customer, both of large revenue.
- $b_o = b_1 = \$52,000$ and $d_o = d_1 = \$250,000$.
- Use loss model 1 (convex decreasing) and $f_o = 1.2$.
- Loss of each insured is log-normally distributed with a mean \$5,965,571 and median \$3,326,313 (NetDiligence 2016-17 report).

	Cases	Median ($)	Mean ($)
Nano Revenue (¡ $50M)	52	49,000	215,297
Micro Revenue ($50M - $300M)	31	88,154	487,411
Small Revenue ($300M - $2B)	15	118,671	599,907
Mid Revenue ($2B - $10B)	9	91,457	173,851
Large-Revenue ($10B - $100B)	8	3,326,313	5,965,571

Numerical Example

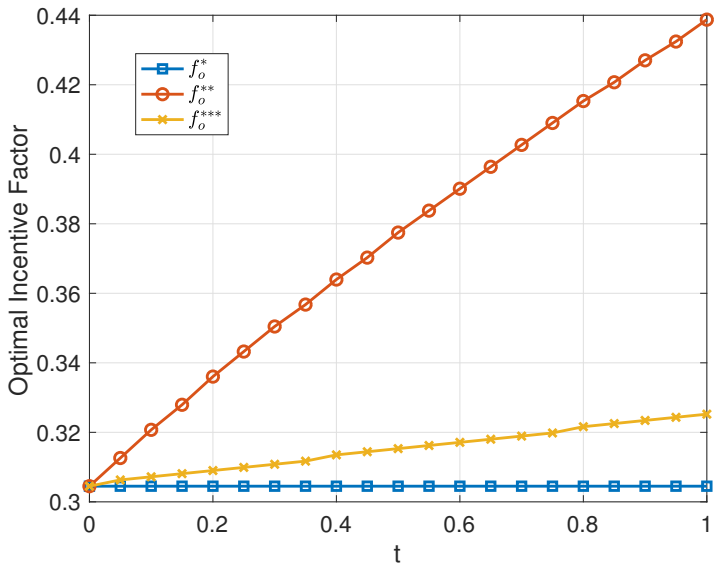


(a) Profit of the insurer ($t = 0.5$)

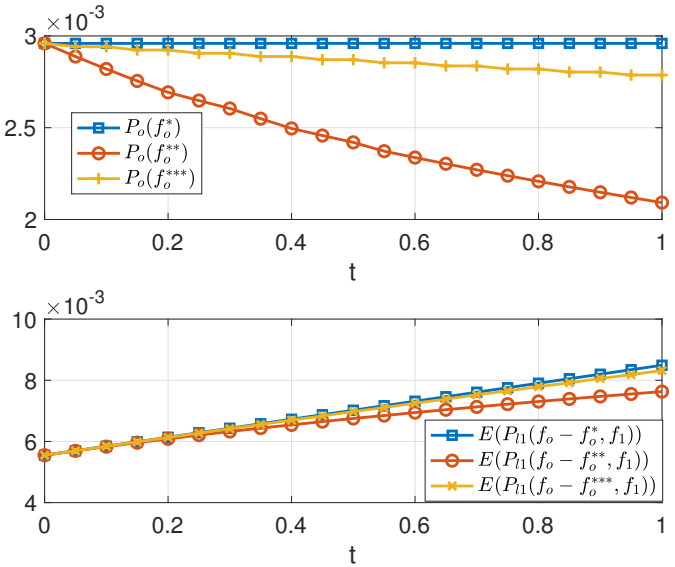


(b) Profit gain as a function of t

Numerical Example



(a) Optimal incentive



(b) Probability of a loss event

Is the premium discount sufficient?

- Consider a non-financial technology service provider firm with annual revenue \$6M.
- Base premium $b_o = \$7,500$.
- We will assume the firm is assessed with $f_o = 1.2$.
- If the insurer sets $f_o' = 0.35$, the SP receives $b_o \cdot 0.35 = \$2,625$ in discount.
- An IT security personnel with a BS degree, 5 years of experience, with salary of \$85K:

$$\frac{\$2625}{\$85000} \times 50 \text{ working weeks} = 1.5 \text{ weeks}$$

- Is this sufficient?
  - Maybe yes, maybe no (it reduces the risk by 10^{-9} (model 2), 0.05 (model 3)).
  - Mismatch could stem from the loss functions.
  - Just as likely: base premiums are out of touch to begin with.

Conclusion

Counter to standard practice, our results show that, by structuring a portfolio that includes both service provider and its customers:

- Security incentives offered to the SP are higher (relative to only insuring the SP or only its customers).
- Overall risk of a loss for the SP and customers is lower.
- Carrier profits are higher.
- Social welfare is higher.

Acknowledgement

Work supported by the NSF and the DHS

References:

- Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, M. Bailey and M. Liu, "Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents", *USENIX Security*, August 2015, Washington, D. C.
- A. Sarabi, P. Naghizadeh, Y. Liu and M. Liu, "Prioritizing Security Spending: A Quantitative Analysis of Risk Distributions for Different Business Profiles", *WEIS*, June 2015, Delft University, The Netherlands; *Journal of Cybersecurity*, December 2016.
- **M. Khalili, P. Naghizadeh and M. Liu, "Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence", NetEcon, 2017; IEEE Trans. Information Forensics & Security (TIFS), February 2018.**
- **M. Khalili, M. Liu, and S. Romanosky, "Embracing and Controlling Risk Dependency in Cyber-Insurance Policy Underwriting", Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria.**