A Research Agenda for Cyber Risk and Cyber Insurance

Preprint · February 2019

DOI: 10.13140/RG.2.2.30462.23367

18 authors, including:

Gregory Falco
Massachusetts Institute of Technology
13 PUBLICATIONS **19** CITATIONS

SEE PROFILE

A Research Agenda for Cyber Risk and Cyber Insurance

By: Gregory Falco, Stanford University

Martin Eling, University of St. Gallen

Danielle Jablanski, Stanford University

Lawrence A. Gordon, University of Maryland

Shaun Shuxun Wang, Nanyang Technological University

Joan Schmit, University of Wisconsin-Madison

Russell Thomas, RMS and George Mason University

Mauro Elvedi, University of St. Gallen

Thomas Maillart, University of Geneva

Emy Donavan, Allianz

Simon Dejung, SCOR Reinsurance

Matthias Weber, SwissRE

Eric Durand, SwissRE

Franklin Nutter, Reinsurance Association of America

Uzi Scheffer, SOSA

Gil Arazi, FinTLV Ventures

Gilbert Ohana, FinTLV Ventures

Herb Lin, Stanford University

Abstract

Cyber risk as a research topic has attracted considerable academic, industry and government attention over the past 15 years. Unfortunately, research progress has been modest and has not been sufficient to answer the "call to action" in many prestigious committee and agency reports. To date, industry and academic research on cyber risk in all its complexity has been piecemeal and uncoordinated – which is typical of emergent, pre-paradigmatic fields. Further complicating matters is the multidisciplinary characteristics of cyber risk. In order to significantly advance the pace of research progress, a group of scholars, industry practitioners and policymakers from around the world present a research agenda for cyber risk and cyber insurance, which accounts for the variety of fields relevant to the problem space. We propose a cyber risk unified concept model that identifies where certain disciplines of study can add value. The concept model can also be used to identify collaboration opportunities across the major research questions. In this agenda, we unpack the major research questions into manageable projects and tactical questions that need to be addressed.

1. Introduction

In today's digitally interconnected environment, every company is now a tech company. Every political entity is now a digitally-enabled one. Therefore, digital or "cyber" risk is business risk. While this may be a provocative statement to some, an irrefutable fact is that digital transformation is accompanied by new organizational exposure that needs to be managed accordingly. To date, efforts to evaluate the complexity of cyber risk have been piecemeal and uncoordinated – not unlike other emergent fields. This is wasting financial and intellectual capital, while also impeding new markets from flourishing (e.g. cyber insurance). The goal of this document is to propose a research agenda for cyber risk that aligns the interests of industry, academia, non-profits, and governments. To be successful, this agenda must resonate with all fields studying cyber risk including data science, behavioral science, economics, computer science, management science, political science, and law.

There are hundreds, if not thousands, of reports, white papers and academic articles that refer to cyber risk. Cyber risk is a multi-disciplinary issue, therefore ownership of cyber risk as a field of study has been decentralized across academic fields that seldom lack coordination. Our agenda's focus is cyber risk management and cyber insurance for firms and similar organizations, individually and also in interdependent networks (e.g. supply and partner networks, critical infrastructure, etc.). This includes relevant government and non-profit organizations. We do not address cyber risk for individual people, nor do we address cyber risk for society at large, including international relations.

Because of the diverse audience for this research agenda, we conducted an extensive feedback exercise where we circulated this document with colleagues across the globe for each aforementioned field of study. The extensive collaborative process in formulating this agenda, reflected by the variety of coauthors, yielded a cyber risk intellectual space for each discipline. As reflected in Figure 1, we developed a *Unified Concept Model for Cyber Risk*. Disciplines will be able to use Figure 1 and the subsequent agenda as a starting point for their cyber risk research, understand how their work fits into the broader cyber risk research landscape and determine which fields could collaborate on certain topics. Figure 1 reflects the primary disciplines that might be engaged for each component of the cyber risk agenda. These primary disciplines are not definitive, but rather a notion of interest by the constituent discipline's reviewers of the agenda and are subject to change.

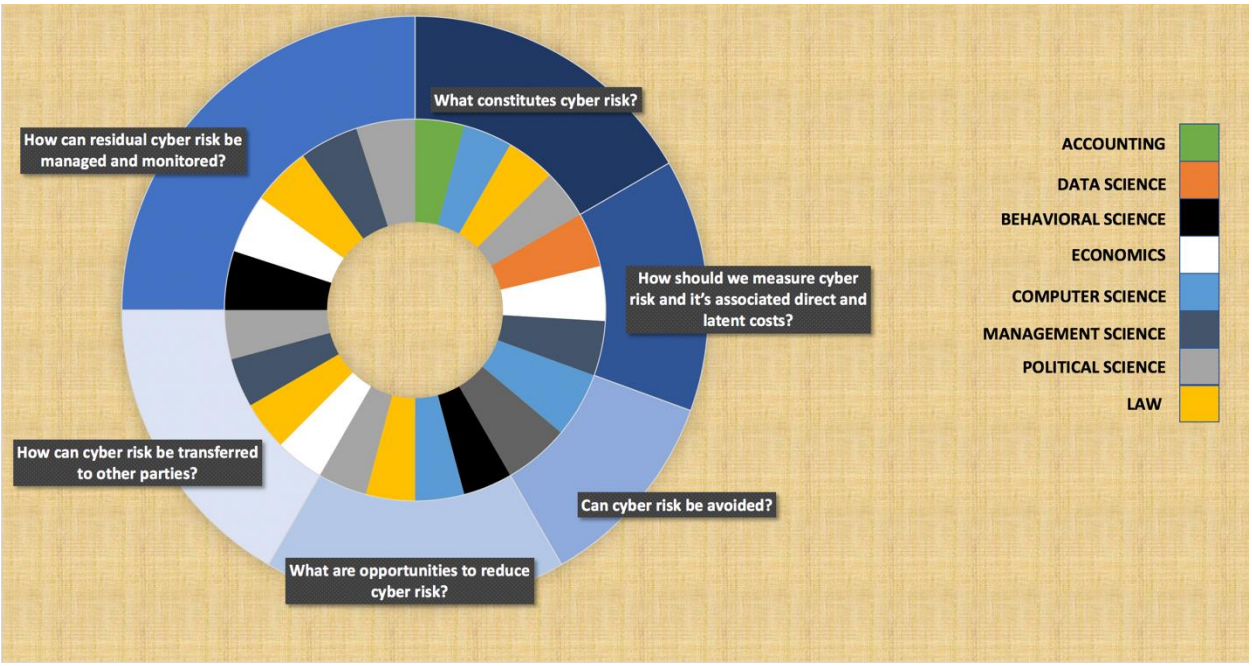

Figure 1 : ***Cyber Risk Unified Concept Model;*** *outer ring displays 6 umbrella questions; inner ring shows potential collaborations on each overarching question between the 8 listed disciplines*

The agenda elaborates on the six big questions identified by the co-authors in the Cyber Risk Unified Concept Model, proposes disciplines that could be well-equipped to study them, unpacks a variety of related, tactical research questions and provides sources as a starting point for each area of focus. The big questions include:

- What constitutes cyber risk?
- How should we measure cyber risks?
- Are there cyber risks that can be avoided?
- What are the opportunities to reduce cyber risk?
- How can cyber risk be best transferred to other parties?
- How can residual cyber risk be managed and monitored?

2. What constitutes cyber risk?

Primary Disciplines: Accounting, Computer Science, Law, Political Science

There is not one single type of cyber risk. Cyber risk could come in the form of unintentional data leakage, privacy loss, malicious attempts to damage digital systems, malicious attempts to steal or alter corporate confidential data for economic advantage or even as disinformation campaigns. The damage could be sporadic or a global damage that affects global digital assets (DDOS). There is an entire spectrum of cyber risk an organization can face ranging from unintentional data leaks to strategic, nation-state attacks. The scope of cyber risk has been difficult to characterize because there is widespread disagreement about what a cyber event actually entails. Some organizations consider a cyber event to be any unknown connection attempt to their network. Others consider successful unauthorized access to their network a cyber event. Still others define a cyber event as an instance when “loss” is experienced. Understandably, it is exceedingly difficult to benchmark security or risk across an industry or even within the same organization if everyone is using different definitions of an

event. This issue is compounded by the varying definitions provided by standardization organizations such as NIST, ISO and MITRE.

For the purposes of establishing a cyber risk body of knowledge, it is vital to have clear and consistent terminology about cyber events and their impact potential. Disparate definitions of a cyber event will limit the ability for consistent reporting and data analysis about cyber risk. Further, it could complicate the ability for research studies to build on each other – one of the fundamental cornerstones of scientific progress.

Further complicating matters, the scale and scope of cyber risk is problematic depending on choice of boundary for data, computing systems, and stakeholders. Moving from narrow to broad, here are alternative scope statements for cyber risk:

- A single organization's cyber risk based on their owned assets.
- A single organization's cyber risk encompassing owned assets, third-party provider assets, public infrastructure (e.g. internet service providers) and its supply chain cyber risk.
- A series of organizations' collective cyber risk that accumulates based on their reliance on a common digital asset (e.g. cloud infrastructure).
- A series of organizations' collective cyber risk that accumulates based on their utility of ubiquitous software that shares a common vulnerability.
- An insurer's or institutional investor's accumulated cyber risk based on outstanding policies and liabilities for interdependent industries or interdependent cyber incidents.
- Reinsurers perspective of cyber risk aggregation and liabilities for interdependent industries or interdependent cyber incidents.
- IoT/SCADA risk as multi-industry catalyzer for cyber risk and attacks.

Cyber risk is fundamentally different than other risks faced by businesses and covered by insurance (e.g. Property & Casualty, Errors & Omissions, etc.) in two ways.

First, the causal factors that drive cyber risk change and evolve rapidly – sometimes in less than a year, which is less than the insurance period for most cyber insurance policies. For a given firm, cyber risk can decrease within the insurance period because new security controls or resources have been successfully deployed, or vulnerabilities reduced, or the attack surface has been significantly reduced. But for that same firm cyber risk increase because attack surface increases, or security controls deteriorate, or new vulnerabilities appear, or because attacker tools and practices have evolved. Changing the IT landscape of an organization (new software used, new integration with suppliers, acquisition of additional companies /integration with such companies' networks)) also increases the cyber risk during the insurance period.

Second, cyber activity does not usually follow clear patterns, which might help estimate the risk. For example, an advanced attacker who is specifically targeting individual organizations will never do the same thing twice. The barrier to modifying an attack is low and since skilled attackers do not want to risk being caught, they change approach. This often makes historical data of little use to assess a future risk.

Regarding cyber events, the time scope (duration) of cyber events and impact is problematic. Unlike perils like car accidents, earthquakes and others, a cyberattack even or episode can last for days, weeks, or months until it is recognized and stopped. Evaluation of the damages can also take long

periods of time, since it is not always known what data was stolen and what uses are planned for the stolen information by the attackers. Cyberattacks can also proceed in stages, either by the same attackers or through other attackers with different resources or objectives, who acquire useful credentials or other data through "black hat" markets.

Regarding cyber loss (i.e. impact, damage), the losses could be sporadic and isolated or it could be global and widespread. It could include only tangible losses or both tangible and intangible damage. A cyber event could be any unknown attempt to a network or device. Or it might be defined to only include successful unauthorized network access. A more narrow definition of cyber event is when an economic loss is realized.

These problematic characteristics can significantly vary across different regions and business sectors, but all are essential considerations in studying cyber risk.

Related tactical questions include:

- What are the different types of cyber events (distinguished by actor, impact, target precision, intent)?
- What are relevant trends with respect to the different types of cyber events?

Potential Research Projects

- Document and analyze the evolution of cyber events in relation to how they have impacted organizations over the years. Identify potential patterns and trends that can be used to project future cyber event threats.
- Assess the determinants of cyber risk and identify any industry differences.
- Assess what constitutes material cyber risk for corporate investors.
- Evaluate how cyber events have and will continue to evolve.

Sources

Böhme, Rainer, Stefan Laube, and Markus Riek. "A Fundamental Approach to Cyber Risk Analysis." Variance Journal, www. variancejournal. org, online edition (2017).

Böhme, Rainer. Towards Insurable Network Architectures (Versicherbare Netzarchitekturen). it - Information Technology 52(5): 290-294 (2010)

Cukier, Kenneth Neil, Viktor Mayer-Schönberger, and Lewis Branscomb. "Ensuring (and insuring?) critical information infrastructure protection." Report of the 2005 Rueschlikon Conference on Information Policy (2005). Retrieved from: https://www.belfercenter.org/sites/default/files/files/publication/rwp_05_055_viktor_branscomb.pdf

CRO Forum. "CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk." (2016).

Department of Homeland Security (US). Cyber Security Research and Development Broad Agency Annoucement (BAA) 11-02 (Solicitation). (2011). Retrieved from: https://www.fbo.gov/utils/view?id=560a331a2f0105f32ca8c1e4f068c5e6

Eling, Martin. "Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research." Geneva Papers on Risk and Insurance 43.2 (2018): 175-179.

Eling, Martin, and Werner Schnell. "What do we know about cyber risk and cyber risk insurance?." The Journal of Risk Finance 17.5 (2016): 474-491.

Fisk, Gina, et al. "Privacy principles for sharing cyber security data." Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015.

Ramirez, Robert, and Nazli Choucri. "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review." IEEE Access 4 (2016): 2216-2243.

Ross J. Anderson: Liability and Computer Security: Nine Principles. ESORICS 1994: 231-245

U.S. Securities and Exchange Commission (SEC) "CF Disclosure Guidance: Topic No. 2" on Cybersecurity Risk and Cyber Incidents (see: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm)

Wang, S., Integrated Framework for Information Security Investment and Cyber Insurance (September 15, 2017). https://ssrn.com/abstract=291867

3. How should we measure cyber risk and its associated direct and latent costs?

Primary Disciplines: Data Science, Economics, Management Science

Establishing consistent metrics that can communicate the extent of cyber risk internally and externally is important to understanding an organization's cyber posture. One of the more important reasons to establish metrics is to understand the cost and benefits of investing in cybersecurity.

There will always be tradeoffs to security. Sometimes, it is convenience, other times it is a direct cost, and in some cases it is technological progress. The many types of tradeoffs can be abstracted into an equation with variables and represented as the level of cyber risk that an organization is comfortable with. Today this equation is formulated ad hoc for individual organizations based on point-in-time data. The calculus is then used to assess how much spending should be done to manage cyber risk. While these cyber risk equations such as presented in the Gordon-Loeb Model could be tactically useful (i.e., for supporting individual decisions), they do not capture macro cyber risk trends that could influence an organization's long-term risk management strategy.

Also, current models fail to capture the considerable interdependencies across digitally enabled systems and their respective industries. The failure or compromise of a single digital system could cause cascading failures and exponential repercussions. This complicates the calculus of an organization's cyber risk. It is unclear where the line should be drawn about where one organization's cyber risk ends and another's begins. These interdependent digital systems lead to one type of cyber accumulation risk.

Accumulation risks for cyber can involve the reliance across several industries on a subset of third-party providers. For example, there is a critical mass of digital capabilities across multiple organizations and industries that are reliant on a handful of cloud service providers. A cloud service provider can be seen as a single point of failure across multiple industries. Should one of these digital infrastructure services be compromised, millions of their users will be

impacted globally.[1] One such example could be for critical infrastructure that operates on supervisory control and data acquisition (SCADA) systems. An attack on a SCADA system that controls the electric grid could have cascading impacts across sectors. As previously mentioned, risk damages can vary from tangible damages as extreme as human life, to intangible assets like reputation damages and financial losses, over a very long period of time.

The metric used to measure cyber risk by data science researchers is frequently considered to be the expected loss from a cyber breach. However, different metrics (e.g., probability of a loss of a given size, variance of potential loss) are sometimes used by researchers in other disciplines.

Methodologies are needed to improve the modeling of interdependent cyber events so that organizations can better prepare for cyber threats across a given industry or several interdependent industries. Further, these models can help evaluate accumulated risk potential. This research could be used by insurers improve estimates risk exposure in portfolios and to define risk tolerances.

Such research could be leveraged by insurers to calculate risk exposures and define risk tolerances.

Related tactical questions include:

- What type of forward-looking accumulating scenarios are conceivable (e.g. (i) one attacker exploits common hardware vulnerabilities, common software vulnerabilities, common procedural design flaws, common human behaviors; (ii) one successful attack on a single company has a ripple effect on many companies, industries; (iii) orchestrated multiple attacks (similar to 9/11);?
- How likely are the accumulation scenarios? What is the severity?
- What are potential interconnections (within / across entities; within / across industries)
- What economic theories can be transferred to analyze cyber risks and which ones are not transferrable?
- What data is needed to reliably assess the performance of a cyber economic model? For example, independent realizations of risk realizations on networks (I.e., many independent networks of comparable type).
- How can cyber risk across interdependent industries be normalized such that we can compare risks across industry?
- How can digital interdependencies be measured?
- How and to what extent, if any, can cyber events be accurately modeled and ultimately predicted considering past attacks are not necessarily indicative of future ones?
- Under what circumstances, if any, are degrees of modeling and prediction possible?

Potential Research Projects

- Define representative extreme– but nevertheless possible – and potentially interdependent and accumulating cyber scenarios, determine associated economic and insured industry losses, and estimate associated probability ranges. (Work in progress at Stanford – working title: Can a Cyberattack Cause a Financial Crises?).

[1] If all of these users had cyber insurance, the effects could be devastating on the underwriters and reinsurers of the policies considering the scale of the accumulated risk.

- Interview cyber insurance providers, , reinsurers and actuaries to understand accumulation scenarios they envision. Assess the adequacy of accumulation scenarios used by the insurance industry.
- Investigate the various applications of economic and statistical models to cyber risk and evaluate their effectiveness. Propose new modeling approaches and existing techniques that appropriately cater to the unique challenges of modeling cyber risk.
- Evaluate the extent of accumulation using a big data/AI platform. (Work in progress at FinTLV Ventures).

Sources

Agrafiotis,I., J.R.C. Nurse, M. Goldsmith, S. Creese, and D. Upton “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate”, Journal of Cybersecurity, 2018, 1–15

Anderson, Ross, and Tyler Moore. "The economics of information security." Science 314.5799 (2006): 610-613.

Bodin, L., L.A. Gordon and M.P. Loeb, “Information Security and Risk Management,” Communications of the ACM, Vol. 51, No. 4, 2008.

Böhme, Rainer, and Galina Schwartz. "Modeling Cyber-Insurance: Towards a Unifying Framework." WEIS. 2010.

Böhme, Rainer, and Gaurav Kataria. "Models and Measures for Correlation in Cyber-Insurance." WEIS. 2006.

Dejung, Simon. “Economic impact of cyber accumulation scenarios.” Swiss Insurance Association SVV Cyber Working Group. (2017).

Eling, Martin, and Jan Wirfs. "What are the actual costs of cyber risk events?." European Journal of Operational Research 272.3 (2019): 1109-1119.

Eling, Martin, and Kwangmin Jung. "Copula approaches for modeling cross-sectional dependence of data breach losses." Insurance: Mathematics and Economics 82 (2018): 167-180.

Eling, Martin, and Nicola Loperfido. "Data breaches: Goodness of fit, pricing, and risk measurement." Insurance: Mathematics and Economics 75 (2017): 126-136.

Falco G., Caldera C. and Shrobe H., "IIoT Cybersecurity Risk Modeling for SCADA Systems," in IEEE Internet of Things Journal. doi: 10.1109/JIOT.2018.2822842 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8332467&isnumber=6702522

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.

Hubbard, Douglas W., and Richard Seiersen. How to measure anything in cybersecurity risk. John Wiley & Sons, 2016.

Maillart, Thomas, et al. "Given Enough Eyeballs, All Bugs Are Shallow?." Revisiting Eric Raymond with bug bounty markets (2016).

Romanosky, S. Examining the costs and causes of cyber incidents, Journal of Cybersecurity, Volume 2, Issue 2, 1 Dec 2016, Pages 121–135

Ruan, Keyun. "Introducing cybernomics: A unifying economic framework for measuring cyber risk." Computers & Security 65 (2017): 77-89.

Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. How bad is it? – A branching activity model to estimate the impact of information security breaches. Workshop on the Economics of Information Security (WEIS), Washington, DC. (2013).

Wang, S., Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain (November 3, 2017). https://ssrn.com/abstract=3064533

4. Can cyber risks be avoided?

Primary Disciplines: Computer Science and Management Science

One of the most under-developed areas of research is cyber risk avoidance, which usually involves managerial decisions at the level of enterprise architecture so that the enterprise is "less risky by design". Of course, the interconnectivity of digital systems today is essential to the success in most industries, and therefore not all cyber risks can be avoided. But too often researchers, industry practitioners, and government policy makers take for granted the unchecked expansion of digital computing, communications, and interconnection.

One mechanism to avoid cyber risks is to minimize the use of computing systems and their connectivity. We do not necessarily encourage this, however, it is indeed a risk avoidance mechanism that some organizations employ. For example, anecdotally, we were informed that in several nuclear facilities, conscious decisions were made to revert to analog devices to avoid cyber risk. This is not a decision to be taken lightly considering the benefits digital devices afford (another, slightly "softer" practice, is to use internet-disconnected networks to reduce risk, like the use in military networks. Conversely, deciding to take such networks offline can generate additional cyber risks associated with off cycle or custom patches or other work necessary to maintain functionality/operability when a network is not readily connected to the internet. The unplugging argument does raise the issue of over-digitization of assets and the inherent cost/benefit of security to convenience and operational efficiency. This becomes an important discussion point for operations managers and those studying digital transformation.

Another option to avoid risk is by designing and using inherently secure systems. Today most devices, networks and systems make use of technology that was built without security as a priority. This issue is now even more pronounced with the prevalence of internet of things (IoT) devices that are designed with low-cost connectivity in mind (by vendors with little experience in the software sector). Some new approaches to designing and building software and hardware systems embody security-by-design principles. Such principles include practices such as deny-by-default where a system inherently disallows processes from running so that the surface area of attack is minimized. The intention of these securely designed digital assets is to optimize functionality while attempting to guarantee some level of security. Further technical advancements in this area—including those that can help to reduce the sometimes exorbitant cost of such assets—will only help to avoid cyber risks to the extent the securely designed systems are deployed. A persistent challenge to realize the benefits of new technology is device lifecycle, where it could be decades (as is the case for industrial systems) before devices are replaced and the security of the system is updated accordingly. Conversely, there is a trade-off:

continuously replacing devices to more modern ones, with security implemented, also imposes the risk of new vulnerabilities detected and exploited, since new devices are using new protocols, new features and functionality, which exposes to new risks.

Matters of risk avoidance fall to system operators who can determine the operational value of having a digitized asset (and therefore judge if a digital system is necessary) and computer scientists that can design inherently secure systems.

Although in defined domains, one can argue that it is a best practice to minimize the use of connected systems, the global trend and development is forcing society the other way – being more connected, using more technologies and producing more data. Most businesses are critically (and increasingly so) dependent on technology and connected channels. Modern life and future trends will dramatically increase our dependence on connected technology (e.g. connected and autonomous cars).

Related tactical questions include:

- What is the utility curve for digital assets when compared with their security tradeoffs?
- What stakeholders need to be involved in decisions regarding averting cyber risk?
- What are new security-by-design principles that can be employed?
- How can accumulation risk be averted?

Potential Research Projects

- Interview organizations that have removed digital assets to avoid cyber risk and derive a list of considerations that could help organizations make similar decisions.
- Research the requirements for and then design an inherently secure industrial controller that can be updated without causing system downtime.
- Evaluate the security of the update process. In many cases, the complexity of the maintenance interface (in order to be secure) exceeds the complexity of the primary application. Establish a standardized update process that maintains security while preserving simplicity.

Sources

Anderson, R., Böhme, R., Clayton, R., and Moore, T. Security Economics and the Internal Market. ENISA, Heraklion, Greece, 2008.

Eling, Martin, and Werner Schnell. "What do we know about cyber risk and cyber risk insurance?." The Journal of Risk Finance 17.5 (2016): 474-491.

Böhme, Rainer. "Cyber-Insurance Revisited." WEIS. 2005.

Kuypers, Marshall, and Thomas Maillart. "Designing Organizations for Cyber Security Resilience." WEIS2018.

Shetty, Sachin, et al. "Reducing Informational Disadvantages to Improve Cyber Risk Management." The Geneva Papers on Risk and Insurance 43.2 (2018): 224-238.

5. Where are opportunities to reduce cyber risk?

Primary Disciplines: Behavioral Science, Computer Science, Law, Political Science

The Parkerian hexad outlines six elements of information security organizations should consider: confidentiality, possession or control, integrity, authenticity, availability and utility. The goal of fending off attacks theoretically entails preserving the hexad. Increasingly, organizations understand that they cannot protect themselves from and prevent all threats all the time. This raises the need to prioritize their systems, networks and data's security and evaluate the opportunity to reduce cyber risk across the security hexad. Further, the relative importance of confidentiality, integrity and availability based on organizational context must be explored.

For example, if an organization faces the threat of a data breach versus data corruption – should one require more attention than the other? Some experts argue that for personally identifiable information (PII), confidentiality should no longer be a security priority because of the many large-scale data breaches that have occurred to date. It is inevitable that personal information will be stolen at some point in today's cybersecurity climate. Therefore, more resources should be expended on authenticating the integrity of personal information through relational information rather than focusing on keeping the information hidden. Of course, these experts would argue that confidentiality should not be ignored, but simply prioritized accordingly. It is important to note, however, that such deprioritization can have regulatory consequences and potentially create economic loss due to fines/penalties (CCIA and GDPR fines for this). Organizations have finite resources available to manage cyber threats. Therefore, to properly manage cyber exposure, it is instrumental to study how organizations should prioritize assets and their associated cyber risks.

Beyond prioritizing and securing the most critical assets, concrete steps towards preventing specific cyber events can also be achieved through threat information sharing. Intra-industry security cooperation could be an effective cyber event prevention tool. The idea behind information sharing is simple. If organization A shares recent attacks with others (B and C) that may use similar digital assets, future attacks against B and C could be prevented. Today, Information Sharing Analysis Centers (ISACs) which have been established to facilitate cyber event information sharing across all critical infrastructure sectors have not been equally successful. ISACs are only as effective as the member organization's participation. Some industries, like the financial sector, have member organizations that actively participate in information sharing. This in turn improves the security posture of the entire industry. Other sectors have seen less member organization participation. Studying why some sectors engage more with their ISACs than others could help improve cyber event prevention in sectors without effective information sharing.

There is a public good character of cybersecurity, which leads to some typical economical underinvestment problems. From an individual's point of view it might be optimal to reduce investments in cybersecurity and public policy might help (or be needed) to get to some minimum standards for prevention. In light of the lack of policy direction in this space, it is important to evaluate market mechanisms that can have the same effect. Cyber insurance can be an example of this.

Some sectors already require insurance for daily operations. If cyber event prevention requirements were incorporated into mandated insurance policies, organizations would need to comply quickly for fear of losing their operating license. Importantly though, requiring purchase of a cyber insurance policy is not the point. Rather forcing a security conversation as part of the underwriting process for purchasing cyber insurance can potentially help institutionalize discussions and practices concerning cybersecurity.

Another market mechanism that some sectors require to indicate a minimum level of security is accreditations and certifications. Accreditations and certifications often require some compliance exercises to maintain status which assumes there is a third-party auditor of security practices that grants credentials. Such program are imperfect because they promote a “checkbox” compliance culture where many organizations stop worrying about their cyber risks if they complete the certification process. For this reason, several market mechanisms are needed to work in concert to reduce cyber risk at scale.

Related tactical questions include:

- How can specific risk related to confidentiality, integrity and availability be reduced? How can the "right" human behavior be achieved?
- Which mitigation efforts make sense based on a cost / benefit analysis?
- Who should be responsible for mitigation?
- Which industries care most about preserving A) Confidentiality, B) Possession or Control, C) Integrity, D) Authenticity, E) Availability, and F) Utility?
- Which industries have a good cyber hygiene? Who is this related to (or caused by) the type of business, market structure, and the regulatory environment? How can this be assessed and monitored?
- What are approaches to determining prioritized assets?
- What data should be used to prioritize assets?
- How do risk assessment tools account for prioritized assets?
- How are shared assets or third-party assets accounted for in prioritizing risk?
- How should cyber policy be enforced?
- Should insurers take on the role of a cyber security standard enforcer?
- Should hardware and software producers be made liable for the cyber risk of their products?
- Should providers of cyber security services be held liable for the quality of their services?
- What other cyber risk practices should be mandatory?
- What would cyber data collection standards look like that can facilitate risk analyses for various purposes (operational risk, insurance underwriting, evaluating impact of cyber hygiene, etc.)?
- What disclosure considerations should be taken into account when sharing anonymized cyber event data?
- Can we build “best practices” to handle companies’ cyber risk?
- What would the role of compliance and regulation should there be a chance for global compliance/alliances?
- What are capital requirements to finance cyber risk?
- What are response and recovery plans?
- What kind of scenario training can be conducted to manage cyber loss events?
- What factors need to be considered for enumerating long-term cyber event consequences?

Potential Research Projects

- Investigate the extent to which cyber security standards should be mandated. Determine if cyber security is considered a public good and understand parallels across industries to other public goods.
- Study the potential unintended consequences of mandating cyber security standards. (Work in progress at University of Innsbruck).

- Explore external incentives for cyber security. Conduct roundtables with industry and policymakers (separately) to understand why today's incentives are insufficient.
- Understand the extent of success ISACs have had today. Determine what makes some work and others less effective.
- Conduct a roundtable of stakeholders such as ISAC organizers, trade associations, think tanks and industry cyber data stewards to determine a data collection standard for cyber risk information, and how such a standard could be implemented. The stakeholders for the exercise should be selected based on the purpose of the data collection standard. Produce a report associated with cyber data practices.
- Interview CISOs to understand how and what cyber data is shared anonymously and determine what information is currently being held back for what reasons (e.g. privacy concerns, reputational preservation, competitive advantage, etc.). Evaluate opportunities to minimize these barriers.

Sources

Anderson, R., Böhme, R., Clayton, R., and Moore, T. Security Economics and the Internal Market. ENISA, Heraklion, Greece, 2008.

Böhme, R. Security Audits Revisited. In A. Keromytis, ed., Financial Cryptography and Data Security. Lecture Notes in Computer Science 7397, Springer, Berlin Heidelberg, 2012, pp. 129–147.

Bandyopadhyay, Tridib, Vijay S. Mookerjee, and Ram C. Rao. "Why IT managers don't go for cyber-insurance products." Communications of the ACM 52.11 (2009): 68-73.

Laube, S. and Böhme, R. Strategic Aspects of Cyber Risk Information Sharing. ACM Computing Surveys (CSUR), 50, 5 (November 2017), 77:1–77:36.

McQueen, Miles A., et al. "Time-to-compromise model for cyber risk reduction estimation." Quality of Protection. Springer, Boston, MA, 2006. 49-64.

Refsdal, Atle, Bjørnar Solhaug, and Ketil Stølen. "Cyber-risk management." Cyber-Risk Management. Springer, Cham, 2015. 33-47.

6. How can cyber risk be best transferred to other parties?

Primary Disciplines: Economics, Law, Management Science, Political Science

Another problematic aspect of cyber risk is accountability and responsibility. There is serious need for more research on how quantified cyber risk might improve accountability and responsibility, and also how it might have undesirable consequences. There are both social and financial definitions an implications of risk transfer. The financial definition of "risk transfer" is "a third-party takes responsibility for uncertain costs or losses, governed by contract, and usually in exchange for a premium or other compensation". Most often the third-party is an insurance company. The societal definition of "risk transfer" is "another party (second, third, …) takes over accountability and responsibility for the uncertain costs, losses, consequences, or remediation efforts." Organizations that have cyber risk transferred to them are subject to social sanctions such as blame, legal liability, etc. but also can claim social responsibility and authority such as leadership, sponsorship, and value network orchestration.

After each cyber event, fingers are pointed within an organization. More often than not, the CISO and/or the CIO take the blame for a cyber event. However, other times a system admin is blamed. In rare cases, where a major cybersecurity breach occurs, the CEO or the board of directors are held responsible for a breach. Ownership of cyber risk within an organization is generally unclear – even if there is a CISO or CIO that is supposed to manage information security. Because cyber risk is a key part

of an organization's overall business risk, cyber responsibility should be distributed across the organization. On a micro level, questions about the role of a CISO, where a CISO should sit in an organization and the extent of responsibility a CISO has is important to understanding an organization's cyber risk.

On a macro scale, it is important to consider how organizations can transfer cyber responsibility and the associated risk externally to insurers, capital markets, contracts in indemnity and hold harmless agreements, or even the government. Today there are clear gaps in understanding how to accurately price the forward-looking cyber risk for a specific organization. There are even bigger gaps in understanding how cyber risks can accumulate across sectors and interdependent assets. This has inhibited the insurance industry from assuming more of this risk. As insurers and reinsurers become more confident in the extent of these risks, insurance can become a greater force in helping organizations transfer cyber risk. The same can be said for capital markets as cyber risk takers. However, there are some cyber events that the private sector may have limited interest in covering. One example is events deemed as "cyberwar".

Beyond assessing defensive responsibility for cyber risk, it is vital to understand the attack dimension as well. Understanding who the adversary is, their motive, the sophistication and the scale of the attack could help to uncover if the attack was an act of war. Conversely, not all cyber risk incurred is the result of a malicious actor, but instead a result of unintentional behavior by people with certain access to network, data and systems. To distinguish the motive is important because at the point a cyber event is considered an act of cyberterrorism or cyberwar, it may become the government's responsibility to interject and help manage cyber risk for private organizations, not dissimilar to what happened after 9/11. Some cyber risks and their associated causes will be easier to insure than others. For example, risks caused by unintentional behavior are typically not systematic and do not accumulate across companies in the same way that a concerted attack may accumulate. Therefore, unintentional behavior-caused cyber risks are likely to be more insurable.

To date many cyber insurance policies contain "acts of war" exclusions. However, there are many cyberwar definitions in use. We expect some of these definitions to change – and possibly consolidate – after a major cyberattack that insurance practitioners consider cyberwar.

Clarification around understanding both defensive cyber risk ownership, attribution and attack context are critical for selecting strategies to manage different cyber threats. A persistently moving target for what is cyberwar will not only hinder the private sector's ability to properly manage their risk, but also limit insurers' interest in covering cyber risk.

Related tactical questions include:

- How and when should cyber risk be transferred to insurance, capital markets or governments?
- Which risk transfer efforts make sense based on a cost / benefit analysis?
- Should cyber exposures be covered by specific cyber insurance policies?
- Where in an organization should cyber risk responsibility, accountability and liability fall?
- How should an act of war be defined for cyber?
- What if there is a string of attacks that together constitute cyberwar, but separately just seem like one-off attacks?

- How and to what extent is it feasible for insurers to provide insurance coverage for certain cyberwar scenarios?

Potential Research Projects

- Determine today's opportunities to transfer risk and the limitations of transferring cyber risk. Identify ways to increase insurability of cyber. Here we can compare cyber risk with other types of risks that have been introduced to the insurance marketplace in the past, such as environmental degradation, employment practices liability, director's and officer's liability, and others.
- Cyberwar and cyber terrorism do not have clear lines in the policy community. Provide a good definition of cyber war, incl. a delineation from cyber terrorism and cybercrime. Evaluate at which point governments must intervene.
- Analyze the economic case for various public/private risk sharing structures for e.g. accumulating cyber scenarios that are (i) too great to be absorbed by the private re-/insurance market, and/or (ii) events with a terrorism- and war-like character

Sources

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. "Insurability of cyber risk: An empirical analysis." The Geneva Papers on Risk and Insurance 40.1 (2015): 131-158.

Bodin, L., L.A. Gordon, M.P. Loeb and A. Wang, 2018. Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy 37(6): 527-544 (see: https://doi.org/10.1016/j.jaccpubpol.2018.10.004).

Eling, Martin, and Jingjing Zhu. "Which Insurers Write Cyber Insurance? Evidence from the US Property and Casualty Insurance Industry." Journal of Insurance Issues 41.1 (2018): 22-56.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. "A framework for using insurance for cyber-risk management." Communications of the ACM 46.3 (2003): 81-85.

7. How can residual cyber risk be managed and monitored?

Primary Disciplines: Behavioral Science, Economics, Law, Management Science, Political Science

Regardless of prevention measures that organizations take, there is still some probability that an organization will experience a cyber event. Responding to residual cyber risk is as important as preventing the risk. There are multiple components of incident response including internal communication, external communication, threat containment, system repair and conducting attack post-mortems. Several organizations believe that upon being attacked, they can call the FBI or some government agency to request help. This is largely a fallacy. As evidenced in several high profile cyber events, incident response is managed by third-party consultants, not the government. Engaging these consultants becomes financially burdensome quickly. Therefore, the financials of residual risk management must be carefully studied.

One major residual risk issue organizations are struggling with is understanding how reputational damages manifest over time after a cyber event. While the stock price implications of a cyber event have been documented thoroughly, reputational damages long-term are less understood which can have indirect impacts on business performance.

Research is needed across the spectrum on residual cyber risks. Operators need better incident response playbooks, to include strategies and plans for communicating with various parties—shareholders, government officials, regulatory authorities, and the public. Executives need a clearer

understanding of how much residual risk will cost and how to account for this in fiscal planning. Each of these areas can be unpacked yielding many interesting projects that can span across disciplines.

Related tactical questions include:

- What are capital requirements to handle residual risk?
- What are potential recovery plans?
- What kind of scenario training can be conducted to manage residual risk?
- What factors need to be considered for enumerating long-term cyber event consequences?

Potential Research Projects

- Evaluate existing scenario trainings for cyber residual risk. Analyze the extent they cover financial risk management versus business continuity.

Sources

Choucri, Nazli, Stuart Madnick, and Priscilla Koepke. "Institutions for cyber security: International responses and data sharing initiatives." Cambridge, MA: Massachusetts Institute of Technology (2016).

Falco, G., Noriega, A., and Susskind, L.. “Cyber Negotiation: A Cyber Risk Management Approach to Defend Urban Critical Infrastructure from Cyberattacks”, The Journal of Cyber Policy. 2019. Doi: 10.1080/23738871.2019.1586969

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. "Sharing information on computer systems security: An economic analysis." Journal of Accounting and Public Policy 22.6 (2003): 461-485.

Romanosky, Sasha, et al. "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?." (2017).

Spanos, Georgios, and Lefteris Angelis. "The impact of information security events to the stock market: A systematic literature review." Computers & Security 58 (2016): 216-229.

8. Conclusion

The main takeaway from this research agenda is the need for a multidisciplinary research approach to the six umbrella questions that make up the Cyber Risk Unified Concept Model and to begin work on the dozens of related empirical questions. As cyber risk as research problem continues to develop it requires shared understanding within and between aforementioned fields, coherence on which disciplines are best suited to tackle specific problem sets, and identification of collaborations with the potential to be most impactful.

Private industry and public organizations will benefit greatly from unbiased efforts to understand cyber risk. Disciplines involved with cyber risk research are tasked with working together while not overstating their own expertise. For example, data scientists need to evaluate the data while political scientists draw inferences from the past and present to lend insight on the cyberwar debate, and so on. Not only will effective multidisciplinary cooperation provide valuable understanding for cyber risk mitigation, but it will also begin to provide unique insights for dealing with cyber incidents. We believe that each discipline has a unique role in helping industry and academia make progress towards understanding cyber risk. Because of cyber risk’s interdisciplinary nature, it is essential for each field to evaluate how they fit into the broader research agenda.