Cyber Protection Strategies: Balancing Insurance and Security

Li Huang and Kimberly Cornell
University at Albany, USA

lhuang9@albany.edu
kacornell@albany.edu

Abstract: Firms employ various cybersecurity measures such as procedural controls, technical measures, and physical installations to mitigate and maintain risk at acceptable levels. The advent of cyber insurance has introduced a new dynamic, potentially discouraging self-protection due to coverage for losses. However, recent trends indicate a shift towards integrating cyber insurance into Information Technology (IT) risk management strategies. Cyber insurance can incentivize firms to optimally allocate security resources, particularly when premiums are tied to a firm's security level. The availability and pricing of insurance coverage reflect an organization's commitment to mitigating potential losses incurred from security breaches. This study examines the impact of cyber insurance on self-protection by developing an expected utility model that combines risk preference and utility theory. The model is contextualized within a monopolistic market scenario with mandatory participation, where organizations must purchase cyber insurance. This compulsion incentivizes firms to enhance their security posture to secure favorable insurance pricing. The study compares risk preferences across different scenarios, both with and without cyber insurance. Our findings show that premium discrimination affects agents differently based on risk preferences. Risk-neutral agents are more responsive to varying premiums, adjusting their investment in preventive measures accordingly. In contrast, risk-averse agents prefer to transfer risk through insurance rather than invest heavily in prevention. The study provides insights into firms' risk management strategies, particularly regarding purchasing cyber insurance and selecting appropriate premium policies. By highlighting how incentive mechanisms like cyber insurance can align IT strategies with the overarching goal of safeguarding cyberspace, this research contributes to understanding behavioral aspects of cybersecurity practices. Moreover, the study underscores the importance of aligning insurance premiums with security investments to create a balanced approach to risk management. By doing so, firms can protect themselves more effectively and contribute to a more secure digital environment.

Keywords: Cybersecurity, Risk preference, Expected utility, Security investment, Cyber insurance

1. Introduction

Effective and efficient cybersecurity practices and policies are essential to our ever-growing digital world. Businesses and social activities increasingly rely on the Internet, enjoying the convenience of emerging technologies. However, this dependency on information and telecommunication technologies heightens potential IT security risks. Malicious activities, including hacking, distributed denial-of-service attacks, phishing, pharming, and the dissemination of viruses and worms, pose significant threats to the integrity, confidentiality, and availability of information (Craigen, 2014). For example, the 2019 Capital One data breach compromised over 100 million customers' personal information. This breach stemmed from a hacker exploiting a misconfigured web application firewall, gaining access to sensitive data, including names, addresses, credit scores, and Social Security numbers. Similarly, the SolarWinds incident allowed hackers unauthorized access to numerous organizations worldwide. These breaches underscore the critical need for prioritizing information protection.

IT risk management extends beyond technological concerns, involving the interplay between people, technology, and information. The 2014 Target data breach, caused by a phishing attack on a contractor, highlights the dangers of inadequate cybersecurity procedures (Lukic, 2020). Cyber insurance is increasingly important in mitigating cyber risks as it can provide access to security services and legal assistance, helping organizations manage cyber risks. Cyber insurance providers often require companies to implement minimum security controls, such as access authentication, thereby reducing overall risk. Cyber insurance influences a firm's security by affecting its decisions regarding its self-protection (Cordell, 2017; Gordon, 2003). The model we develop in our study assumes that participation in cyber insurance is mandatory and that the cyber insurance market is monopolistic. This approach is taken to eliminate the need to consider moral hazards (Lelarge and Bolot, 2009; Yang and Lui, 2014; Kesan, Majuca, and Yurcik, 2005).

This study explores the relationship between cyber insurance and self-protection, focusing on risk preferences. We aim to understand how cyber insurance affects security practices and contributes to risk management strategies.

2. Concepts

2.1 Risk

Risk has a multi-fold definition: it refers to the effect of uncertainty on objectives (Aven, 2013). It can be an uncertain event that negatively impacts the achievement of objectives (Aven, 2013; Galway, 2004). Risk is a security challenge. It emphasizes uncertainty and possibility and adversely influences some endeavors. Risk is described as a combination of likelihood and consequences, where the likelihood is devoted to the threat level and existing vulnerability (Bouveret, 2018). Risk can be expressed as the possible negative consequences (harm) weighed by the probability of occurrence (D. W. Woods and Böhme, 2021). Therefore, cyber risk is defined as the likelihood of a successful cyber-attack and the potential harm to digital assets (Nurse, Creese, and De Roure, 2017).

2.2 Risk Management

Scholars define risk management as assessing risk, reducing risk to an acceptable level, and maintaining risk by not exceeding that level (Gordon, Loeb, and Sohail, 2003). The first step is risk assessment, which is identifying, quantifying, and estimating risks to assets and internal operations (Nurse et al., 2017). Cyber risk assessment includes the identification of threats and vulnerabilities, quantifying cost and value, and estimating investment returns. Risk assessment can also be called risk analysis as it involves identification, quantification, and security investment analysis. However, risk management depends on risk analysis to devise an effective strategy. Risk analysis quantitatively or qualitatively estimates uncertainty and impact, and risk management practices the developed strategy to ameliorate the identified risks (Galway, 2004). Risk management involves approaches against risks. Noticeably, the concept of risk management indicates that the goal of management is not to eliminate risks but to reduce and maintain risks to a tolerable level. There are several approaches to achieving this goal, and one such approach is security investment. Security investments refer to the money spent on security solutions (antivirus, firewall, detection system, etc.) to secure cyber security over a period with the expectation of risk reduction (Lee, 2021). Scholars and practitioners focus on a risk-based benefit – the reduced uncertainty in expected loss due to a security breach (Arora, Hall, Piato, Ramsey, and Telang, 2004). The returns from security investments provide information for an optimal investment plan.

Cyber risk management entails limiting data access to avoid putting sensitive data at risk, including assessing risks, reducing risks, and maintaining the risk level (Kejwang, 2022; Gordon et al., 2003; Guttman and Roback, 1995). Risk management is not solely about avoiding or preventing all risks; security solutions also cannot entirely avert cyber risks due to the rapid evolution of technologies. Moreover, preventing all risks is more expensive than accepting some risk damages (Arora et al., 2004). Risk management consists of a series of steps: risk assessment, risk reduction, residual risk maintenance, etc. Risk management does not gain profit but keeps cyber risks aligned with risk expectations. Optimizing risk management is to reduce the expected losses, not only relating to costs but also the return rate - how much incremental returns each additional unit of investment brings. IT managers have two options: self-investment and cyber insurance. There is a trade-off between the amount a firm self-invests and the amount it spends on cyber insurance (Gordon et al., 2003). Their self-investment will decrease as they allocate more of their security budget to cyber insurance. The increased costs associated with cyber insurance may decrease investment in security equipment or software. Managers must consider a strategic and long-term plan determining the amount spent on each part. Self-investment and security practices will improve information security (Anderson and Moore, 2006; Gordon and Loeb, 2002; Kunreuther and Heal, 2003). However, security investment in technologies and infrastructure does not guarantee risk reduction and prevention efficiency. Security solutions cannot provide absolute security for an organization. Damages due to false rates cause financial losses. IT managers may choose to transfer risks to insurance companies.

Frameworks are developed to address the evolving threat landscape and cyber-attack complexity, offering guidance and tools for effective risk management. There are several widely recognized cyber management standards that organizations can adopt to prevent and effectively respond to cyber incidents. These standards offer structured approaches to incident handling and management, providing organizations with guidance on effectively preparing for, detecting, responding to, and recovering from cyber incidents. Organizations select frameworks that best align with their needs to enhance incident response and protect digital assets. The table below summarizes information from various sources, including government reports on standards adopted by international and national organizations and industry documents on risk management best practices.

Table 1: Cybersecurity Frameworks

Name	Key Words
NIST (2024): Cybersecurity Framework	Identify, Protect, Detect, Respond, and Recover
ISO/IEC 27001 (2022): Information Security Management Systems	Identify, Assess, Manage Information Security Risks, Incident Response, and Recovery Procedures
SANS (2011): Cyber Incident Handling Steps	Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
ITIL (2019): Incident Management	Identify, Categorize, Prioritize, Timely Manner, Minimize Impact
CREST (2014): Cybersecurity Incident Management Capability	Prepare, Respond, Follow Up
ISACA (2012): Cyber Incident Management Life Cycle	Plan and Preparation, Detection, Containment, Analysis, Tracking, Incident disclosure
ENISA (2010): Cyber Incident Handling Process	Report, Registration, Resolution, Disclosure, Post-assessment
CERT/CC (2003): Cyber Incident Life Cycle Process	Report, Analyze, Assistance, Coordinate, Resolution
CERT-RMM (2016): Resilience Management Model	Multiple Domains, Respond, Recover
CIS (2021): Internet Security Controls	Control, Vulnerability Assessment, Remediation, Configuration
Kindervag (2016): Zero Trust Model	Control, Monitor, Prevent, Minimize
MITRE ATT&CK (2013)	Mapping, Categorize, and Respond
FAIR (2005): Factor Analysis of Information Risk	Quantify, Assess, Prioritize, Mitigate, Allocate
CMMC (2019): Cybersecurity Maturity Model Certification	Certify, Maturity, Respond

2.3 A dichotomy of Cyber Risk Management

Cyber insurance has evolved from traditional IT company insurance to cover any technology-related losses. Full coverage compensates for data loss regardless of its cause (Talesh, 2018). It offers first-party and third-party coverage. First-party coverage reimburses losses from data breaches and cyberattacks, including theft of trade secrets and hacker extortion (Low, 2017; Gordon et al., 2003). Third-party coverage protects against liability for losses to others (Dambra, Bilge, and Balzarotti, 2020), covering claims from external parties regarding the insured's actions (Romanosky et al., 2019). This encompasses costs like virus transmission, product delivery failures due to hacking, copyright infringement, and expenses for public relations, IT forensics, crisis management, customer breach notifications, credit monitoring, and reputation restoration efforts (Kshetri, 2018). Thus, cyber insurance mitigates various risks and compensates for damages from breaches, extortion, and viruses. However, it cannot cover all losses due to rapidly evolving threats, and its high costs reflect a lack of actuarial data and proper models (Böhme et al., 2010).

Investing in security solutions and cyber insurance involves a trade-off. More extensive security measures typically reduce insurance coverage (Huang, Siegel, and Madnick, 2018). This balance affects the residual risk, which comprises the risks remaining after implementing security solutions. Cyber insurance compensates for the damage related to these residual risks, potentially impacting the financial resources allocated for security investments aimed at minimizing risks. Therefore, a benefit-cost analysis can incorporate the relationship between risk reduction and financial protection.

2.4 Risk Preference

Risk preference dictates allowable residual risks. Risk appetite shows the willingness to accept dangers for certain values (Aven, 2013), indicating the risk level an entity tolerates to pursue goals. A low appetite indicates acceptance of minimal risk, while a high appetite reflects a readiness to endure more. Risk appetite can be risk-seeking or risk-averse (Aven, 2013; Berlinger, 2015). An entity evaluates options by the expected utility to find an optimal choice (Dou et al., 2020). Risk-averse agents prioritize reducing uncertainty in expected loss, leading to higher expected utility from security. They face diminishing marginal utility as the impact of security investment decreases. For risk transfer, risk-averse agents pay more for insurance than the expected loss (Khalili et al., 2019). Risk-neutral agents pay premiums equal to or less than the expected loss (Khalili et al., 2019). Thus, purchasing cyber insurance depends on the utility of expected loss, not merely the loss itself.

Risk management aims to reduce and maintain security uncertainty at a tolerable level (Gordon L. A., 2003). Suppose optimal choice is a function of risk preference λ. Risk preference affects the level of security effort. A firm would like to spend money ahead to prevent certain risk occurrences. However, managers may not have the expertise or knowledge to know how many resources should be allocated for a given situation. As situations

vary, industry standards cannot provide a specific optimal plan for each company. Expected utility theory accounts for risk preferences in decision-making processes (Bolot, 2009; Lelarge, 2009). The final investment depends on the probability and expected utilities for each option. When companies invest in security solutions beyond their needs, they waste money on security investments. Scholars and practitioners can determine optimal investment combination plans and management strategies based on expected utilities to feasible options.

3. Literature Review

Several studies have explored the economics of cybersecurity management. Gordon and Loeb (2002) developed a model for determining the optimal amount to invest in information security. They found that the optimal investment amount is generally much less than the expected loss from a security breach. Building on this, Huang et al. (2008) introduced the idea of "return on security investment" (ROSI), providing a quantitative approach to assessing the value of security measures. However, as Magnusson et al. (2007) pointed out, calculating ROSI remains challenging due to the difficulty quantifying security investment benefits. The implementation of cybersecurity frameworks has also been studied. Jalali et al. (2019) found that while frameworks like NIST provide valuable guidance, many organizations need help with practical implementation, particularly aligning security investments with business objectives.

Cyber insurance is increasingly becoming one component of cyber risk management (Efe and Kazdal, 2019; Cordell and Langdon, 2017). Cyber insurance is supposed to play a role in regulating cybersecurity activities. Unlike traditional insurance products, cyber insurance has specific challenges. For instance, cyber insurance industry and the market lack well-developed mechanisms to assess actuarially and price cyber risks (Kshetri, 2018). Even though some insurers practice discrimination premiums or deductibles for each policyholder, the practices do not settle the problems. Calculating premiums for cyber insurance is challenging (Low, 2017). Moreover, cyber insurance challenges are multi-dimensional, technical, and managerial (Ganapati, Ahn, and Reddick, 2023). There needs to be more comprehensive regulation in the United States of the insurance marketplace. Challenges and threats make it questionable whether cyber insurance can improve cybersecurity.

The question of whether cyber insurance improves cybersecurity has been explored in existing literature. Some scholars argue that cyber insurance can help companies survive data breaches (Lemnitzer, 2021; Cordell and Langdon, 2017). Cyber insurance is designed to pay for data breach-related losses, such as service disruption losses, the cost of notifying customers, scrutiny and fines, and reputation recovery advertisement fees. With insurance reimbursement, businesses have financial resources to pay the loss and recover new business. Cybersecurity insurance can increase users' welfare (Shetty et al., 2010). Cyber insurance can save businesses from cyberattacks and help enterprises recover quickly from data breaches. Cyber insurance keeps business continuous.

After a cyber-attack, business operations will be interrupted due to service or financial chain interruption. Cyber insurance will provide recovery financial assistance for the insured to restore their operations. Moreover, insurers offer some security services. Cyber insurance companies actively assist the insured in complying with privacy laws and dealing with cyber theft (Talesh, 2018). For instance, they provide a set of training menus for employees' training programs, which will improve the organizational capability for any potential cyber risks. They also provide the insured with legal assistance if any data breaches occur. Those services will improve the insured's security and thus defend against potential attacks. The effects of cyber insurance are essential to small and medium-sized businesses (Lemnitzer, 2021). Those companies do not have enough resources, and the support from their insurer will determine whether they can recover from the cyberattacks. Businesses can enhance their security by utilizing the security services provided by the insurance company. A company must improve its cybersecurity standards to secure a favorable premium before purchasing insurance. Post-purchase, the insurer provides guidance on maintaining and updating security systems, enhancing the company's cybersecurity. Thus, cyber insurance promotes best practices in cybersecurity.

Some studies argue cyber insurance fails to improve cybersecurity (Singh and Akhilesh, 2020). Even though it can increase the insured's security posture, cyber insurance has little effect on network security (Shetty et al., 2010). Cybersecurity insurance will decrease the security investment of companies (Pal et al., 2014; Acturia; D. Woods et al., 2017; Gordon et al., 2003; Kunreuther and Heal, 2003). Clients may be less willing to invest in their cybersecurity protections when the insurance will cover potential losses. Once a company buys the insurance, the insurance company will pay the cyber-related loss. The insured will lose the incentive to improve security standards or self-invest in the security system. Even though insurers provide cybersecurity services in their

premium costs, few insureds will use them. So, the insurance will have a negligible effect on security improvement.

The second problem is that cyber insurance companies do not have enough historical data to evaluate potential risks. It is hard to set up proper premiums for individual clients (Kshetri, 2018; Toregas and Zahn, 2014; Granato et al., 2019; Dambra et al., 2020; Gordon et al., 2003). Applying a standard model to all users may overcharge some customers, discouraging them from buying the insurance. Another problem is the need for predictive models for writing and pricing policies for newly emerging cyber risks (Farao et al., 2020). Cyber insurance cannot cover all the losses as cyber threats evolve quickly. Some newly emerging threats are not included in existing insurance coverage. In some situations, the insurance company may refuse to pay for claims because the insured did not meet some pre-requirements. Thus, decision-makers must carefully evaluate the benefits and risks before purchasing cyber insurance products.

Several researchers have explored the impact of risk preferences on cybersecurity decision-making. Hsu et al. (2015) found that risk-averse managers often invest more in cybersecurity measures, while risk-neutral managers are more likely to rely on cyber insurance. However, Dutta and McCrohan (2002) argued that many organizations fail to make rational decisions about cybersecurity investments due to cognitive biases and a limited understanding of cyber risks.

Existing literature offers insights into the relationships between cybersecurity investments, cyber risk management, and cyber insurance; however, gaps remain. First, there is limited empirical data on the long-term effects of cyber insurance on organizational security practices. Second, there is insufficient research on how risk preferences affect the balance between self-protection and insurance in real-world scenarios. More integrated approaches that examine how risk preferences and the availability of cyber insurance affect security investment decisions within the context of recognized cybersecurity standards and frameworks are needed.

4. Proposed Model

Now, we present a model that examines the relationship between cyber insurance and security investment, moderated by risk preference.

Table 2: Cyber Insurance and Risk Metrics

Variable	Range	Description
Security Investment (SI)	$0 \le SI \le 1$	SI represents the percentage of the overall budget allocated to cybersecurity measures. A higher value indicates a greater allocation of resources to cybersecurity
Cyber Insurance Coverage (CIC)	$1 \le CIC \le 10$	A scale from 1 to 10 representing the range of cyber insurance coverage, with 1 indicating the lowest level and 10 the most comprehensive coverage.
Risk Preference (RP)	$1 \le RP \le 5$	A scale from 1 to 5 quantifying risk preference, with 3 indicating risk-neutral, 1 risk-averse, and 5 highest risk tolerance.
Cybersecurity Posture (CP)	$1 \le CP \le 5$	A scale from 1 to 5 quantifying a firm's cybersecurity defense strength, with 1 indicating basic defenses and 5 indicating cutting-edge advantage.

The model proposes that CP=f(SI,CIC,RP) where f is a function such that:

1. To express the effect of SI on CP, we use $f_1=a*\log(SI+1)$. Here, a is a constant that scales the impact of security investment. This means that CP increases with SI, indicating increased security investment leads to improved cybersecurity posture but with diminishing returns.
2. To explain the impact of CIC on CP, we use $f_2=b*CIC-c*CIC^2$, where b and c are constants that determine the peak and the rate of decline. The relationship between CP and CI is non-linear, which means cyber insurance's effect on cybersecurity posture follows an inverted U-shape curve.
3. To examine the influence of risk preference on the effects of SI and CIC, we use $f_3=d*RP$, where d is a constant that adjusts the influence of risk preference. RP moderates the impact of SI and CI on CP.
4. Therefore, the overall cybersecurity posture can be expressed as:

$$f_4=f_3(RP)*(f_1(SI)+f_2(CIC))$$

Function f_4 captures the idea that the cybersecurity posture is influenced by security investment and cyber insurance, with risk preference moderating their effects. Higher or lower risk tolerance may affect how effectively these resources enhance a firm's overall cybersecurity resilience. For instance, firms with lower risk tolerance may favor self-protection measures over cyber insurance to enhance their security. In contrast, those with higher risk tolerance might prefer using insurance as a risk transfer tool. Risk-averse firms are more likely to opt for higher coverage levels. when deciding to purchase cyber insurance. In contrast, risk-seeking firms may prefer more flexible coverage, depending on premium costs.

4.1 Data Description

Given the constraints in data availability, no dataset is available that fully aligns with the proposed model. We plan to collect data through a survey focusing on organizations' information security investment and adoption of cyber insurance products. An ideal dataset will include three primary components. First, cybersecurity investment will be measured by the percentage of an organization's total budget allocated to IT security. This proportion indicates cybersecurity activity within the organization and is commonly used as a measure of investment in cybersecurity (Gordon et al., 2004). Second, the survey will use a binary variable to indicate whether the organization has purchased cyber insurance. Additionally, data on coverage extent and type will be gathered, allowing for analysis of how insurance coverage affects security portfolios. Third, the survey will include data on the organization's level of victimization, quantified by the number of cyberattacks experienced by the organization. Furthermore, we explore the organization's risk propensity by interviewing managers and using their risk attitudes to reflect its overall risk preference.

To better illustrate the characteristics of the ideal dataset, we use the R programming language to randomly generate numerical values representing a diverse range of organizations. We show an example of applying this data generation—to randomly generate 100 companies and assigning each company an industry type. Random values are generated for security investment, cyber insurance coverage, risk preference, and cybersecurity posture. The dataset includes companies from various industries, such as Finance, Manufacturing, Healthcare, and Retail. It reflects real-world scenarios in which cyber attackers target various industry sectors. Table 3 shows a few rows of synthetically generated data, and Table 4 shows each variable's spread and central tendency.

Table 3: Synthetic Data

Company	Industry	SI	CIC	RP	CP
Company_1	Finance	0.16002919	5.946584	1.161950	4.633339
Company_2	Manufacturing	0.17258457	5.337833	1.164345	5.000000
Company_3	Finance	0.07552437	2.435229	4.817737	1.000000
Company_4	Finance	0.19170805	2.346211	2.493365	5.000000
Company_5	Healthcare	0.09404358	5.493456	4.225679	3.966477
Company_6	Retail	0.07236081	9.465084	4.640236	1.000000

Table 4: Descriptive Statistics

Variable	Length	Class	Mode	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
Company	100	chr	chr	N/A	N/A	N/A	N/A	N/A	N/A
Industry	100	chr	chr	N/A	N/A	N/A	N/A	N/A	N/A
SI	N/A	num	N/A	0.05263	0.07895	0.11706	0.12049	0.16137	0.19948
CIC	N/A	num	N/A	1.021	2.808	4.614	5.108	7.451	9.917
RP	N/A	num	N/A	1.066	1.882	2.931	2.291	3.852	4.921
CP	N/A	num	N/A	1.000	2.214	3.482	3.361	4.535	5.000

- Security Investment varies across companies, ranging from 0.05263 to 0.19948. The moderate range between mean (0.120) and median (0.117) represents a relatively symmetrical distribution.
- Cyber Insurance Coverage shows significant variation, from about 1.021 to 9.917, which means from minimal to comprehensive coverage. We can observe positive skewness because the mean (5.108) is larger than the median (4.614). The skewness in distribution represents a long right tail, which means there are more companies with lower coverage while there are few companies with very high

coverage. Considering the increasing costs of cyber insurance premiums, the skewness reflects real-world scenarios.

- Risk Preference varies from 1.066 to 4.921, which indicates risk-averse to risk tolerance. The generated data presents the full spectrum of risk attitudes: the mean is 2.921, suggesting a slightly risk-neutral tendency; the median is 2.931, indicating symmetric distribution.
- The Cybersecurity Posture scale ranges from 1 to 5, meaning from basic to leading-edge. The 1st Quartile, 2.214, and the 3rd Quartile, 4.535, show a good spread.

5. Conclusion

This study examines the effects of risk preference and cyber insurance availability on security efforts. It assumes all agents invest in security due to fixed-value loss, with a firm's risk appetite dictating its tolerable loss level. Rational agents maximize their utility from security or insurance. The analysis reveals that risk preference influences how cyber insurance impacts security efforts. Companies generally adopt a balanced cybersecurity approach, with average values close to the mid-range. Risk-averse agents tend to invest more in security than risk-neutral agents when uninsured, regardless of threat levels. Once cyber insurance is available, risk-averse agents will likely purchase it to handle its residual risks. However, risk-averse agents are less sensitive to changes in premiums.

This study emphasizes cyber insurance's role in fostering responsible cybersecurity practices, guiding IT managers and policymakers in effective cybersecurity strategies balancing self-protection and insurance. However, it relies on theoretical models that may not reflect real-world complexities. Future research should incorporate empirical data to validate these theories. Empirical studies could clarify relationships between risk preferences, security investments, and cyber insurance. This research enhances understanding of how financial instruments like cyber insurance encourage firms to be more responsible for cybersecurity, highlighting the need to align insurance premiums with security investments to manage risks effectively. Future studies will explore interactions between dependent agents influencing cyber insurance choices and investigate security interdependence among agents, testing changes in self-protection and cyber insurance under varying risk preferences.

Acknowledgement

This project was supported by the University at Albany.

References

Anderson, R. and Moore, T., 2006. The economics of information security. *Science*, 314(5799), pp.610–613.

Arora, A., Hall, D., Piato, C., Ramsey, D. and Telang, R., 2004. Measuring the risk-based value of IT security solutions. *IT Professional*, 6(6), pp.35–42.

Aven, T., 2013. On the meaning and use of the risk appetite concept. *Risk Analysis*, 33(3), pp.462–468.

Berlinger, E., 2015. Risk appetite. *Pénzügyi Szemle/Public Finance Quarterly-Journal of Public Finance*, 60(1), pp.49–62.

Böhme, R. and Schwartz, G., 2010. Modeling cyber-insurance: towards a unifying framework. In: *WEIS*.

Bouveret, A., 2018. Cyber risk for the financial sector: A framework for quantitative assessment. *International Monetary Fund*.

Cavusoglu, H., Mishra, B. and Raghunathan, S., 2004. A model for evaluating IT security investments. *Communications of the ACM*, 47(7), pp.87–92.

CERT/CC (2003). *Cyber Incident Life Cycle Process*. CERT Coordination Center. Available at: https://apps.dtic.mil/sti/trecms/pdf/AD1146052.pdf.

CERT-RMM (2016). *Resilience Management Model*. CERT. Available at: https://insights.sei.cmu.edu/library/cert-resilience-management-model-cert-rmm-version-12/.

CIS (2021). *Internet Security Controls*. Center for Internet Security. Available at: https://www.cisecurity.org/controls.

CMMC (2019). *Cybersecurity Maturity Model Certification*. Department of Defense. Available at: https://dodcio.defense.gov/cmmc/About/.

Cordell, D.M. and Langdon, T., 2017. Curbing client risk with cyber insurance. *Journal of Financial Planning*, 30(2), pp.34–35.

CREST (2014). *Cybersecurity Incident Management Capability*. CREST. Available at: https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Maturity-assessment-tool_Info1.pdf.

Dambra, S., Bilge, L. and Balzarotti, D., 2020. SoK: Cyber insurance–technical challenges and a system security roadmap. In: *2020 IEEE Symposium on Security and Privacy*, pp.1367–1383.

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X. and Hu, C., 2020. An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, *527*, pp.576-589.

Efe, A. and Kazdal, H., 2019. IT security trends for e-government threats. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 3(2), pp.105-110.

ENISA (2010). *Cyber Incident Handling Process*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/ce2010report.

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

FAIR (2005). *Factor Analysis of Information Risk.* FAIR Institute. Available at: https://www.fairinstitute.org/what-is-fair.

Farao, A., Panda, S., Menesidou, S.A., Veliou, E., Episkopos, N., Kalatzantonakis, G., … and Xenakis, C., 2020. SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In: *Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17*. Springer International Publishing, pp.65-74.

Galway, L., 2004. Quantitative risk analysis for project management. *A Critical Review*, WR-112-RC. Available at: http://www.rand.org/pubs/working_papers/2004/RAND_WR112.pdf.

Ganapati, S., Ahn, M. and Reddick, C., 2023. Evolution of cybersecurity concerns: A systematic literature review. In: *Proceedings of the 24th Annual International Conference on Digital Government Research*, pp.90–97.

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

Gordon, L.A., Loeb, M.P. and Sohail, T., 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3), pp.81–85.

Granato, A. and Polacek, A., 2019. The growth and challenges of cyber insurance. *Chicago Fed Letter*, *426*, pp.1-6.

Guttman, B. and Roback, E., 1995. An introduction to computer security. *National Institute of Standards and Technology Administration US*.

Hausken, K., 2006. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, 8, pp.338–349.

Huang, C.D., Hu, Q. and Behara, R.S., 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International journal of production economics*, *114*(2), pp.793-804.

Huang, K., Siegel, M. and Madnick, S., 2018. Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys*, 51(4), pp.1–36.

ISACA (2012). *Cyber Incident Management Life Cycle*. ISACA. Available at: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance.

ITIL (2019). *Incident Management*. AXELOS. Available at: https://www.itlibrary.org/index.php?page=Incident_Management.

Jalali, M.S., Siegel, M. and Madnick, S., 2019. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), pp.66-82.

Kejwang, B., 2022. Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. *International Journal of Research in Business and Social Science (2147-4478)*, 11(6), pp.334–340.

Kesan, J., Majuca, R. and Yurcik, W., 2005, June. Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study. In *Proc. WEIS* (pp. 1-46).

Khalili, M.M., Liu, M. and Romanosky, S., 2019. Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, *5*(1), p.tyz010.

Kindervag, J. (2016). *Zero Trust Model*. Forrester Research. Available at: https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf.

Kshetri, N., 2018. The economics of cyber-insurance. *IT Professional*, 20(6), pp.9–14.

Kunreuther, H. and Heal, G., 2003. Interdependent security. *Journal of Risk and Uncertainty*, 26, pp.231–249.

Lee, I., 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), pp.659–671.

Lelarge, M. and Bolot, J., 2009, April. Economic incentives to increase security in the internet: The case for insurance. In *IEEE INFOCOM 2009* (pp. 1494-1502). IEEE.

Lemnitzer, J.M., 2021. Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, 6(2), pp.118–136.

Low, P., 2017. Insuring against cyber-attacks. *Computer Fraud & Security*, 2017(4), pp.18–20.

Lukic, D., 2020. Target Data Breach: How Was Target Hacked? *IDStrong*. Retrieved June 11, 2024, from https://www.idstrong.com/sentinel/that-one-time-target-lost-everything/.

Magnusson, C., Molvidsson, J. and Zetterqvist, S., 2007, May. Value creation and return on security investments (ROSI). In *IFIP International Information Security Conference* (pp. 25-35). Boston, MA: Springer US.

MITRE ATT&CK (2013). *MITRE ATT&CK Framework*. MITRE Corporation. Available at: https://attack.mitre.org/.

NIST (2024). *Cybersecurity Framework*. National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework.

Nurse, J.R., Creese, S. and De Roure, D., 2017. Security risk assessment in Internet of things systems. *IT Professional*, 19(5), pp.20–26.

Pal, R., Golubchik, L., Psounis, K. and Hui, P., 2014. Will cyber-insurance improve network security? A market analysis. In: *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp.235–243.

Romanosky, S., Ablon, L., Kuehn, A. and Jones, T., 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), tyz002.

SANS (2011). *Cyber Incident Handling Steps*. SANS Institute. Available at: https://www.sans.org/white-papers/1516/.

Shetty, N., Schwartz, G., Felegyhazi, M. and Walrand, J., 2010. Competitive cyber-insurance and internet security. In: *Economics of Information Security and Privacy*, pp.229–247.

Singh, A. and Akhilesh, K., 2020. The insurance industry—cyber security in the hyper-connected age. *Smart Technologies: Scope and Applications*, pp.201–219.

Talesh, S.A., 2018. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, 43(2), pp.417–440.

Toregas, C. and Zahn, N., 2014. Insurance for cyber attacks: The issue of setting premiums in context. *George Washington University*.

Woods, D., Agrafiotis, I., Nurse, J.R. and Creese, S., 2017. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1), pp.1–13.

Woods, D.W. and Böhme, R., 2021. SoK: Quantifying cyber risk. In: *2021 IEEE Symposium on Security and Privacy (SP)*, pp.211–228.

Yang, Z. and Lui, J.C., 2014. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, pp.1-17.