Quantification of Cyber Risk for Actuaries

An Economic-Functional Approach

Executive Summary

Quantification of Cyber Risk for Actuaries

An Economic-Functional Approach

Executive Summary

Unal Tatar — University at Albany – SUNY, Albany, NY, USA

Omer Keskin — Old Dominion University, Norfolk, VA, USA

Hayretdin Bahsi — Tallinn University of Technology, Tallinn, Estonia

C. Ariel Pinto — Old Dominion University, Norfolk, VA, USA

Project funding from the following organizations:
Casualty Actuarial Society
Canadian Institute of Actuaries
Society of Actuaries

Caveat and Disclaimer

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries or its respective members. The Society of Actuaries makes no representation or warranty to the accuracy of the information

Quantification of Cyber Risk for Actuaries

An Economic-Functional Approach

Executive Summary

Section 1: Introduction and Overview

Because of its complexity, ensuring the security of cyberspace is one of today's most significant challenges. As the cyber environment becomes more integrated with the real world, the direct impact of cybersecurity incidents on business is also heightened. Cyber risk analysis is the primary tool for managing the consequences of cyber events.

Risk analysis is conducted by answering three questions:

1. What can go wrong?
2. What is the likelihood of it happening?
3. What is the impact if it happens? (Kaplan and Garrick, 1981)

Based on these questions, the general formula of quantitative risk analysis, which also applies to cyber risk analysis, is created. According to this general formula, the risk is a set of triplets: $R = \{< S_i, P_i, X_i, >\}, i = 1,2,..,N$, where S_i is a scenario identification, P_i is the probability of that scenario, X_i is the impact which occurs in this scenario, and N is the number of scenarios considered (Kaplan and Garrick, 1981).

Cyber risk is defined by the National Institute of Standards and Technology (NIST) as "risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system" (Stouffer et al., 2019).

Impact assessment, as an integral part of risk analysis, tries to estimate the possible damage of a cyber threat on a business or mission. It provides insight into risk prioritization as it incorporates business requirements into risk analysis for a better balance of security and usability. Furthermore, this assessment constitutes the main body of information flow between technical people and business leaders. It therefore requires effective harmonization of technological and business aspects of cybersecurity (Bahsi et al., 2018).

1.1 Limitations of current cyber risk analysis methods

Current cyber risk analysis methods have several limitations. Cyber risk is often treated as an information technology problem rather than a vital part of enterprise risk management (Moore, Dynes, and Chang, 2015). Existing cyber risk analysis methods assess risk mostly at the asset layer (i.e., assessing software, hardware, data risks via software quality assurance, vulnerability analysis, intrusion detection, malware analysis), to some degree at the organization level (i.e., business processes), and very infrequently at the ecosystem level (i.e., supply chains) (U.S. Department of Homeland Security, 2018).

Another deficiency is the insufficiency of the metrics used to support investment decisions, including cyber insurance, security, and controls. Qualitative metrics and operational terms, rather than quantified financial measures, are often used as cyber risk indicators that guide investment decisions. Qualitative or operational cyber risk metrics lead to 1) a lack of understanding on the part of organizational leaders, and 2) a reluctance to appreciate the significance of cyber risks. This issue was stated in the Strategic Plan for the Federal Cybersecurity R&D Program: "There is no scientific basis for cost risk analysis, and business decisions are often based on anecdotes

or unquantified arguments of goodness" (National Science and Technology Council, 2011). Besides this, the lack of quantification of how investments in specific controls change risk level (i.e., measurement of the effectiveness of planned or implemented controls) is another limitation of current cyber risk analysis methods.

The language used in the communication of cyber risks between cybersecurity decision-makers across management levels and operating units of an organization varies. Decision making in cybersecurity, like many other areas, is accomplished at three levels: tactical, operational, and strategic. The difference in the decision-making parameters of tactical (e.g., the number of vulnerable systems), operational (e.g., legal and organizational constraints), and strategic (e.g., impact on overall business) level managers creates a communication gap, which prevents an accurate assessment of cyber risk.

The impact and likelihood of a risk scenario can differ over time. Temporal change of strength and criticality of dependencies and the associated risk value are covered in very few studies.

The goal of this research is to build a probabilistic, quantitative cyber risk analysis model on how cyber risk on assets relates to organizational goals. In this method, we will consider the cascading impacts through the internal dependencies of an organization.

The developed cyber risk analysis method employs probabilistic attack graphs, that are based on known vulnerabilities in computer software and network topologies. The dynamic risk assessment capabilities are augmented in the attack graph using Bayesian networks. The proposed framework will also leverage the functional dependencies. The cyber impact propagation is modeled within the layers of an enterprise and among different enterprises. Features include expressing impact as a function of loss of confidentiality, integrity, and availability (CIA), and new mathematical dependency relations reflecting the nature of cyber dependencies. Definitions to keep in mind are as follows:

- *Confidentiality* is "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" (McCallister, Grance, and Scarfone, 2010).
- *Integrity* is "the security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation)" (Stoneburner, 2001).
- Availability is "ensuring timely and reliable access to and use of information" (Ross, McEvilley, and Oren, 2016).

Loss of CIA is measured in this study to quantify the impact of cyber-attacks on enterprise systems. Further analyses quantify the economic impact using the loss of CIA.

This study aims to develop a generic model that can be applied by any organization. For the validation of the developed cyber risk analysis method, simulations and sensitivity analysis will be performed.

1.2 Cyber risk management from an actuarial perspective

Actuaries perceive cyber risk management as a problematic issue. In conventional insurance, historical data about claims are commonly preferred for use in actuarial models. In the cyber domain, however, there is a lack of historical data for two main reasons: (1) cyber insurance is a relatively new and novel area where there is no long history going back decades and (2) the existing data quickly becomes obsolete since the threats, vulnerabilities and mitigation methods develop rapidly (Böhme, Laube, and Riek, 2017).

Some studies in the literature aggregate the currently available cyber incident loss data to come up with an average total loss (Biener, Eling and Wirfs, 2015; NetDiligence, 2018). However, their outcomes are not beneficial because the methods and contexts of the studies vary significantly. While Biener, Eling and Wirfs (2015) suggest the average cost per cyber incident is $40 million over 994 incidents between 1971 and 2009, NetDiligence (2016, 2018) concludes a $0.7 million average cost over 1,201 claims between 2013 and 2017. The two previously mentioned reasons may explain such differences. These issues cause concerns for actuaries trying to use this kind of data in analyses. The context of each cyber incident may be significantly different in addition to the differences among various enterprises from different industries.

The issues with data-dependent cyber risk modeling have forced actuaries to look for alternative approaches for estimation of loss modeling and cyber risk quantification. The developed model in this study helps actuaries evaluate the cyber risks an enterprise information and communications technology (ICT) network poses in order to come up with well informed decision making for policy coverage, premiums, and deductibles. This model can be applied to any enterprise ICT network by customizing the inputs accordingly.

1.3 Contributions

The scientific contributions of this research centers around its pursuit of better understanding and improved assessment of impact in the context of cyber risk analysis. One of the most innovative outcomes is the development of a quantitative, graph-based, probabilistic risk model to determine impact propagation within each layer and among all layers (i.e., asset, service, or business process layer) of an organization.

This method evaluates the steps of attacks and assesses how other components are affected by connecting common vulnerability scoring system (CVSS) powered probabilistic attack graphs and functional dependency networks. The proposed method helps to prioritize vulnerabilities based on the impact they cause and to promote better risk-informed investment decisions.

This report is available in English only at this time. The French version will be available over the coming months. A French version of the executive summary is available.