FEATURE

Understanding Cybersecurity Risk

Progressive organizations know that risk is a fact of business. More than that, they recognize the need for integrated and sustainable solutions to address critical operational failures. A broader understanding of security-related risk adds value to an organization. Strong protection of data, infrastructure, personnel and other main resources helps improve regulatory compliance and manage external threats. Modern organizations should view risk and security challenges as opportunities to gain a competitive business advantage. Proactive organizations that have a strong information security footprint that is directly connected with the organization's business strategy, products and IT function will deliver on their toughest challenges and drive growth.

Sound security means protecting the confidentiality, integrity and availability (CIA) of the organization's data while making information accessible. The same also applies to cybersecurity, as it is all about protecting the organization's digital assets from information security breaches and protecting data in electronic form at all times.

Syed Alay Raza, CISA, CRISC, CRMA
Is a chief information security officer (CISO) and head of the information security division (risk management group) at National Bank of Pakistan, the largest government bank in Pakistan. He has significant experience in technology governance, information security, risk management and project management in the financial, commercial and public sectors. He has also worked extensively with international development agencies on multiple technology transformation initiatives.

Currently, many organizations are facing multiple cyberthreats including malware, spoofing, website hacking, spam, phishing emails, denial-of-service (DoS) and distributed DoS (DDoS) attacks. Due to the increasing sophistication of these cybercrimes, recognizing and evaluating security risk scenarios are very complex, and it is necessary to understand how technologies can be abused. Therefore, there is a strong need to develop a cybersecurity risk model based on factors such as the threat landscape, vulnerabilities, likelihood of a breach and the relevant impact.

Cybersecurity Risk and Uncertainty

In risk management, the definition of "risk" is well known. It is associated with monetary loss due to an incident or event.

For example, if a bank has given loans of US $1 million to agricultural borrowers and there is a 10 percent chance of default, based on the risk pattern of the particular industry and geographical territory, then the monetary value of the risk is a US $100,000 loss to the bank.

Applying the classic model of risk management to cybersecurity risk management is rather difficult due to the major factor that is uncertainty. Information security professionals cannot predict with accuracy the probability and magnitude of cybersecurity-related incidents. They are likely to struggle to estimate the damage that can be caused due to any cybersecurity incident. Uncertainty plays a major part, as no one can accurately guess the damage/data breach inflicted by the hacker. For example, if the emails of an organization's chief executive officer (CEO) or other C-level executives are hacked and leaked, the impact may entail legal proceedings, financial repercussions and resignations or some lesser ramifications, depending on the nature of the leaked data.

Countering Uncertainty With Certainty: A Model-Based Approach

There are widely used and well-tested models available for financial, market and insurance risk. However, operational risk models are quite complicated, and the challenge is selecting the most appropriate quantitative model based on proper understanding of risk and controls. Similar problems have been faced by information security professionals when designing and implementing new cybersecurity risk models using statistical and mathematical approaches such as game theory[1] and fuzzy logic.[2]

> “PROVIDING GAME THEORY TRAINING TO CYBERSECURITY PROFESSIONALS AND EVEN COMMON USERS MAY HELP CREATE AWARENESS ABOUT PERSISTENT CYBERTHREATS.”

Many readers may be familiar with the 2001 US film *A Beautiful Mind*,[3] which focused on John Nash, a professor of mathematics who won the Nobel Prize in Economics for his contributions to a complex concept called game theory. The hypothesis of Nash equilibrium is one of the relatively new approaches to help improve cybersecurity resilience.

In simple terms, a game consists of three sets of elements:

1. Players
2. Actions that are strategies and options available to each player
3. A settlement/consequence that is a function for each player

Game theory helps to detect the threat in order to build strong defenses since it is preventive by nature by predicting the outcome. Providing game theory training to cybersecurity professionals and even common users may help create awareness about persistent cyberthreats. In game theory, currently the most broadly used method of predicting the outcome of a strategic interaction is the Nash equilibrium. The games can be simultaneous or sequential. The elements of a game are:

- Players
- Strategies
- Payoffs
- Information
- Timing

Simple methods of game theory can help predict an array of threats. The assumptions to find solutions are based on the following:

- Rationality and common sense
- Knowledge and information
- Communication through actions

The key game theory implication that cybersecurity professionals can use is to ascertain the best attack and defense strategies assuming that the attackers are aware of the defense mechanisms. As mentioned previously, game theory’s main purpose is to create awareness of different possible attacks with the help of training.
Broadly, there are two classifications of games: static and dynamic. To keep it simple, this article focuses on the basics of static games, which are based on the following conditions regarding information:

- Complete imperfect information
- Incomplete imperfect information

Complete imperfect information is mostly the computational approach of devising the best strategy of the players in a quantitative form. An example of this may be the interaction of cyberattackers and firewalls/intrusion detection systems (IDS) in place, using probability/stochastic games to defend. Incomplete imperfect information is a systematic approach to understand and infer the attacker’s intent and approach. An example is a model that illustrates the interaction of

cyberattackers with cybersecurity professionals, having finite or infinite steps in a repeated game.[4]

Using game theory in cybersecurity can improve the security and resilience of cyberdefense mechanisms. Employing game theory to detect threats will, ultimately, help to build a strong cyberdefense.

Fairly recently, dark web markets have become quite popular. The dark web is a part of the World Wide Web that requires special software to enter. Most websites in the dark web are not indexed by search engines. The game theory approach can also help find information on attackers from the dark web in addition to finding information from conventional sources. The dark web has information about many exploits, including zero-day exploits.

There have been many articles written on the applications of game theory related to information security such as Game Strategies in Network Security[5] and Game-theoretic Foundations for the Strategic Use of Honeypots in Network Security.[6]

Another prominent approach to modelling cybersecurity risk is the fuzzy logic theory which applies to uncertainties in cybersecurity weaknesses and threats and uses fuzzy linguistic variables that represent real-life business environment decision-making to model assessment techniques.

Mathmetician Lotfi A. Zadeh introduced fuzzy logic and the fuzzy set theory in 1965. His original theory on fuzzy sets was based on mathematical analysis with logical implications on risk management.[7] The approach is different from the probability theory and other statistical models as fuzzy logic theory shows the likelihood of truth in an obvious manner while integrating the information in linguistic terms. Fuzzy logic models are more convenient for incorporating different expert opinions and more adapted to cases with insufficient and imprecise data. They provide a framework in which experts' input and experience data can jointly assess the uncertainty and identify major issues.[8]

Information security professionals can create models for cybersecurity risk analysis and develop the functional layers of threats, vulnerabilities, risk and controls. Cybersecurity risk factors deal with the possibility of loss of confidentiality, integrity and availability of data due to any specific threat or organization's vulnerabilities on a given asset.

"FUZZY LOGIC MODELS ARE MORE CONVENIENT FOR INCORPORATING DIFFERENT EXPERT OPINIONS AND MORE ADAPTED TO CASES WITH INSUFFICIENT AND IMPRECISE DATA."

Changing Scenarios

With the advent of the current millennium, there has been a stronger need to ensure that information governance-related policies, processes and controls are implemented by organizations to manage cybersecurity risk. Policies, processes and controls that address cybersecurity risk also tackle a plethora of information security risk; therefore, the terms "cybersecurity" and "information security" are often used interchangeably.[9]

The general public is also recognizing that the Internet is becoming an increasingly intimidating and destructive place, not only for personal online activities such as social media and emails, but also for data in the corporate world. Any breach of personal data impacts the public directly, as personal data reside within government agencies, private firms and financial institutions.

Eric Schmidt, executive chairman of Alphabet Inc., calls the Internet:

> *A network of networks, a huge decentralized web of computer systems designed to transmit information using specific standard protocols. What the average user sees as websites and applications, for example, is really the flora and fauna of the Internet. Underneath, millions of machines are sending, processing and receiving data packets at incredible speed over fiber optic and copper cables.*[10]

New threats are emerging daily from unknown locations (with strange names and even stranger *modus operandi*) and are exploiting the

vulnerabilities of interconnected systems through the Internet and intranet for unlawful and spiteful reasons.

As organizations have become more aware of the problem, they have started gradually using the term "cybersecurity" instead of "information security." This is the first step toward accepting the new and potentially disastrous risk inherent in doing business in today's world. Organizations have to progressively develop more effective and more targeted processes and controls to respond to the risk. This requires board members and senior management to think well beyond the traditional IT areas of networks, applications and data stores.[11]

The risk related to the direct implications (legal point of view) of cybercrimes is far more than the simple information security-related risk. In addition to C-level executives, the cyberincident reporting workflow should include immediately informing legal counsel once the organization faces a cyberattack.

Conclusion

The threat landscape is expanding rapidly in both magnitude and complexity. At present, cyberthreats such as viruses, malware and ransomware are intimidating both organizations and individuals alike.

As a complement to probability and stochastic models that already exist, both game theory and fuzzy logic models can be applied to assess risk for which there are insufficient data and incomplete knowledge. Both game theory and fuzzy logic provide frameworks in which subjective, quantitative and partial information can be used for risk analysis.

Cybersecurity is a multifaceted function that requires domain knowledge as well as discerning abilities to determine possible threats from the large amount of data that are in enterprise networks. Strengthening the security and resilience of cyberspace has become a strategic factor. Game theory and fuzzy logic models are relevant for detecting threats as well as preventing them from occurring.

> "ORGANIZATIONS HAVE TO PROGRESSIVELY DEVELOP MORE EFFECTIVE AND MORE TARGETED PROCESSES AND CONTROLS TO RESPOND TO THE RISK."

Endnotes

1 Myerson, R.; *Game Theory: Analysis of Conflict*, Harvard University Press, USA, 1997
2 Novak, V.; I. Perfiljeva; J. Mockor; *Mathematical Principles of Fuzzy Logic*, Kluwer Academic Publishers, Netherlands, January 1999
3 Universal Studios and Dreamworks LLC, *A Beautiful Mind*, USA, 2001
4 Chukwudi, A. E.; E. Udoka; I. Charles; "Game Theory Basics and Its Application in Cyber Security," *Advances in Wireless Communications and Networks,* vol. 3, no. 4, 2017, p. 45-49, *http://article.sciencepublishinggroup.com/pdf/10.11648.j.awcn.20170304.13.pdf*
5 Lye, K.; J. Wing; "Game Srategies in Network Security," School of Computer Science, Carnegie Mellon University, Pennsylvania, USA, May 2002
6 Kiekintveld, C.; V. Lisy; R. Pibil; *Cyber Warfare: Building the Scientific Foundation*, edited by Jajodia *et al*., Springer International Publishing, Switzerland, 2015
7 Shang, K.; Z. Hossen; "Applying Fuzzy Logic to Risk Assessment and Decision-Making," CAS/CIA/SOA Joint Risk Management Section, November 2013, *https://www.soa.org/research-reports/2013/research-2013-fuzzy-logic/*
8 *Ibid*.
9 American Institute of Certified Public Accountants, "SOC for Cybersecurity: Information for Organizations," *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations.html*
10 Schmidt, E.; J. Cohen; *The New Digital Age: Reshaping the Future of People, Nations and Business*, Hachette, USA, 2013
11 *Op cit* American Institute of Certified Public Accountants