Istanbul Journal of Innovation in Education
Volume 1 Issue 1 January, 2015 pp. 1-13

Cynefin Framework for Decision Makers for Information Systems Security in the face of Information Asymmetry

Mehmet S. DERİNDERE*, İstanbul University
Önder GÖÇER, İstanbul University

Abstract: This conceptual paper examines the dichotomy of IS decision makers as both being the client to security systems providers and provider of security for the established platform and offers Cynefin framework for sense-making in guidance for management decision making landscape. Cynefin framework which was developed in knowledge management context provides a suitable tool of sense-making for decision makers in use of security systems governance whom must both be able to select the right mindset, systems and tools, and also facilitate security using these systems in many cases without adequate knowledge about their internals as well as the environmental factors.

Keywords: Cynefin framework, information asymmetry, complexity, Information Systems, IS security, management ontology, epistemology

Introduction

In the novel Perfume: The Story of a Murderer by Patrick Süskind the protagonist Jean-Baptiste Grenouille murders virgins in search of the "perfect scent", which he finds in a young woman named Laure, whom his acute sense of smell finds in a secluded private garden in Grasse (Süskind, 1985). Following a series of murders which totals to 24 before Laure, Laure's father pieces together the pattern of murders and realizes that Laure who is the most beautiful and beloved young woman in the city is most likely to be the next victim. He flees with Laure to hide and protect her. Using every kind of precaution and diversionary tactics he can think of, changing schedules in the last minute, announcing that they are going to someplace and diverting to another, changing disguises he tries to outsmart the murderer. However, since it never occurred to him that the murderer would be using his nose to track them down, every precaution in the end is for nothing and Laure is killed; her scent is captured.

* Contact Author: mehmetderindere@istanbul.edu.tr, İstanbul, Turkey

Providing security for IS systems is like securing a beloved treasure from a band of bandits whose modus operandi is in many times a mystery to the guardians. Cybersecurity which is a relatively new concept in security has less regard to traditional forms of threats and methods of protection is the new landscape, which even the most able bodied institutions and experts have difficulty to comprehend. The recent leak of NSA files (Greenwald, 2013) from the best protected IS of the intelligence agency and the revelation of Turkish Prime Minister's phone taps from the secure government telecommunication systems (Ajans, 2014) shows the size of the problem which in many cases goes beyond the capabilities of best sourced national institutions.

Cybersecurity is expensive. In a survey of 172 of Fortune 500 companies, it was understood that, by spending $5.3 billion per year on cyber security only 69% of attacks were stopped. In order to increase the rate of success in diverting the attacks to 95%, the spending should be raised to $47 billion (Bloomberg, 2012). Malicious hacking, computer viruses, spyware, phishing, and security backdoors providing unauthorized parties full access etc. are issues that any computer used faces in a daily fashion (Hasan & Kazlauskas, 2009). With all the effort, research, huge budgets of governments and corporations, high alert levels, and highly trained security professionals it is accepted that no human designed system is "secure".

Lack of high-level overall understanding of the human and cyber systems within security is an issue makes it impossible to attain the level of security which ensures the survivability and effective working of human designed systems in many cases. In the core of designing security systems and providing security or lack of thereof is understanding the nature and reality or ontology of such systems. The security of information systems is a "wicked problem" (Chang, 2013). This means that it is a problem, which is ill-defined, difficult, or impossible to solve, because of the incomplete, contradictory, and continuously changing requirements which even makes recognition of the issue problematic (Rittel & Webber, 1975). Since the contingencies which designers and security experts face have no definitive formula and no stopping rule, most of them are unique leaves even the

most well-known threats go unnoticed and unchallenged. There are no immediate or ultimate test of the developed solutions, no true or false, and each solution may have unintended consequences, which may lead to more severe problems, further in time and space. Furthering the problem, there are many times strict political, social, time, and cost constraints (Ackoff, 1974).

This paper approaches the problem of IS from the decision makers perspective and provides a unifying framework to the ontology of the governed systems, both as a customer for security systems whether it is obtained from outside vendors, or developed within and as a service provider for its service users thus becoming the responsible for the security. As a theory for explaining (Gregor, 2006) this paper uses Cynefin framework for making sense through haze of complexity and incomprehensibility in this kind of state within which decisions makers must continuously ensure survival and goal attendance.

Noticing Information Asymmetry Inherent in the Management Landscape

Information asymmetry exists in transactions, where one party has more or better information than the other. Neo-classical approach to economics assumes perfect information for both parties, which means they know everything required in making a rational or profit-maximizing decision. In actual cases there are things that we don't know and things that we don't know that we don't know (Epstein, 1984). What we don't know creates a power imbalance in transactions and whereas many times the contracts fail and sometimes the market fails; meaning goods and services are not efficiently served in free market. Some consequences of information asymmetry in contracting can be given as adverse selection, moral hazard, winners curse, and information monopoly.

George Akerlof in his paper "The Market for Lemons" discussed the information asymmetry in the context of used car market (Akerlof, 1970). A lemon is an American slang term for a cart that is found to be defective, only after it has been bought and cherry for a good used car. The quality of the car, which we can define as "known unknown", is not known by the

buyer. Since many important mechanical parts are hidden from the view and are not easily accessible by the buyer, the buyer doesn't know whether the car is a cherry or a lemon. So all the buyer has as the idea about the car is, it is of average quality, so he is willing to pay only the price for a known average quality car. Since owners of high quality cars know the quality, they rightfully demand a higher price but this means that the best cars don't get sold because, buyers who are unable to distinguish a quality and not so good cars are unwilling to pay the higher price. So the quality cars are no longer offered for sale. Markets get into a vicious cycle, since the average quality of the cars falls down the amount customers are willing to pay fall down and the upper quality of existing market is pulled from the market and so on. At the end, only the lemons are left at the market. So it can be summarized that in a market where the seller has more information about the product than the buyer, bad products can drive the good ones out of the market. In many cases the information asymmetry between the decision makers and the vendors is enough to prevent the decision maker to distinguish a functionally secure product from an insecure one. How can one distinguish the better of two computer security systems, which are marketed with the assertion of having same features? Information asymmetry is not restricted to contracts and can be applied to other aspects of life.

Owner of the IS as the customer

A cyber-security problem is a conflict-resolution scenario that typically consists of a security system and at least two decision makers – the defender and the attacker – that can have competing objectives (Jones, 2013). The defender is interested in the performance of the system security over time, for example ensuring that the system operates at or above some threshold level of performance. The attacker may aim ensuring the system operating below that threshold, but also to access systems undetected and to provide restricted information etc. The aim of cyber-attack may be fear factor aiming to create fear, spectacular factor creating negative publicity for the defender or positive publicity for the attacker, or exploiting vulnerabilities to serve purposes of the attacker.

The methods and technologies available to attackers are almost endless. They can be in the form of physical attacks, social engineering attacks (Murphy, 2011), Denial of Service (DoS), spoofing, sniffing, cookies, viruses, worms, Trojan horses, buffer-overruns, password-thefts, information leaks, zero-day attacks, etc. The cyber threats are unlike any stereotypes of past threats and cyber-attacks are increasing threat to sovereign ability "to pursue national security objectives at both the strategic and tactical levels" (USNI, 2010). Sun Tzu recommends "know thy enemy" but decision makers in many cases are no longer dealing with a known enemy or even a group of known enemies on known battlefields or security domains. The cyber actors which can be found in a wide spectrum from individuals to nation states can be corporations, criminals and criminal enterprises, terrorist and also thrills, or fame seeking parties. The increasing pressure to enlarge the cyber presence for organizations also increases the "surface area" which is exposed to threat.

The status-quo in the security community is observed to have a reactive mindset. Meaning a method of attack is developed and performance of counter-measure is developed to that particular or similar attack generally only after the defending parties notice that something is wrong within the system. Even in this kind of security scenarios the shortcomings of the reactive mindset is evident, when the attacker party uses more advanced and persistent approaches the reactive mindset becomes the constraint on behalf of the defenders. Proactive approaches with actionable cyber-attack forecasting is developed (Jones, 2013) with the objective or learning an attackers behavioral models, to predict future attacks, and selecting appropriate countermeasures, to prevent future attacks using modeling attacker intrusion-detector interaction (Alpcan & Başar, 2006) using stochastic (Markov) game, Nash and Bayesian Equilibria (You & Shiyong, 2003) the issue with depending on prediction and forecasting still remains.

The Cynefin Framework

Cynefin (pronounced kun-ev'in) framework developed by Dave Snowden is a holistic sense-making framework (Kurtz & Snowden, 2003). Cynefin is a Welsh word which is almost impossible to translate into

English. Roughly, it means a passionate connection with a particular place (although commonly it is translated as 'habitat'). Cynefin consists of five domains (Snowden, 2013) that are epistemological paradigms representing various states of reality-sensing. The domains are separated by the way of cause and effects are related or separated.

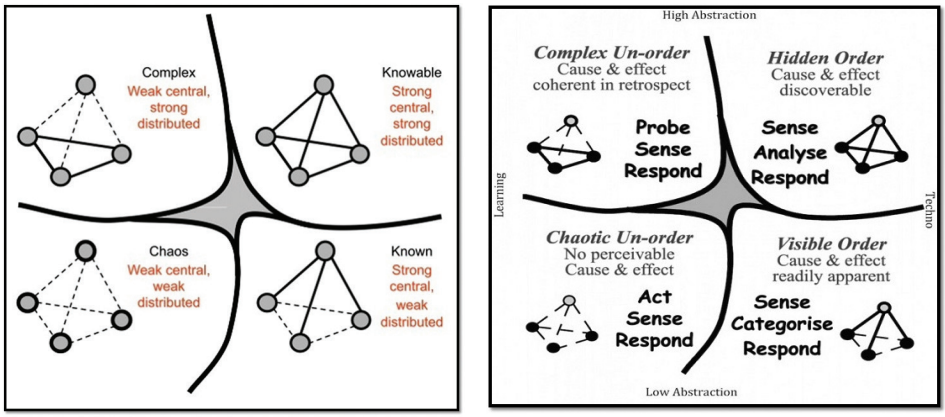
- Simple (known) domain: This is the domain within which the cause and effect relationships are obvious to all. It is presumed that if cause A exists, effect B will certainly be observed. The approach used for decision making and action is Sense- Categorize-Respond which consists of sensing the situation, categorizing the state with a previously developed or learning categories, and responding in a predetermined way.
- Complicated (knowable) domain: In this domain the cause and effect are separated by time and space but through investigation and expert knowledge these relations can be revealed. An example to this domain would mostly be scientific research or complicated machinery, which requires an expert for intervention. The approach best suiting is Sense-Analyze-Respond. After the relationships are well understood, "good" practices are applied.
- Complex domain: The cause and effect relationships in this domain can only be perceived in retrospect or hindsight. They are unknown in advance, thus making planning useless. A model for this domain can be a jungle with thousands of different organisms, their subsystems, systems, complex relationships, dynamic balance, and interactions. No amount of research or exploration can surface all the workings and dynamics of the system, making expertise on the system impossible. One can learn to survive in the system but system dominance impossible without destroying the balance. The proper approach is Probe-Sense-Respond and uses multiple safe-to-fail experiments to allow emergent practices. Complexity Adaptive Systems Theory developed in Santa-Fe Institute, which examines the "complex macroscopic collection" of "similar and partially connected micro-structures", is an example for the systems in complex domain. These systems are complex because they are

dynamic networks of interactions and their relationships are not aggregations of the individual static entities.

- Chaotic Domain: When there is no system level relationship between cause and effect, the domain is called chaotic. This is the domain of novelty within which the best approach is Act-Sense-Response. The chaos theory which originates from the work of Edward Lorenz and examined in great detail especially in mathematical disciplines are relevant in this domain (Kellert, 1993). Organizations in the chaotic state have weak connections with the individuals and social artifacts.

Other than these four main domains there is also a domain named Disorder. Within this domain there is no way to infer the causality type, thus there is no best approach. The interesting aspect of the disorder domain is that every individual tries to apply the approach he is most comfortable within this domain. Whereas those who are "comfortable with stable simple domain try to create or enforce rules, experts seek to conduct research and accumulate data, politicians try to increase the number and range of their contacts, and the dictators eager to take advantage of a chaotic situation seek absolute control. The stronger the importance of the issue the more people seem to pull it towards the domain, where they feel most empowered by their individual capabilities and perspectives" (Kurtz & Snowden, 2003).

Figure 1: Representations of the Cynefin framework domains. (The shaded area in the middle representing the disorder. Strengths of cause-effect connections are shown on the left and proper approaches for domains on the right.)



An example on Mapping Security Issues on Cynefin; The Case of Passwords

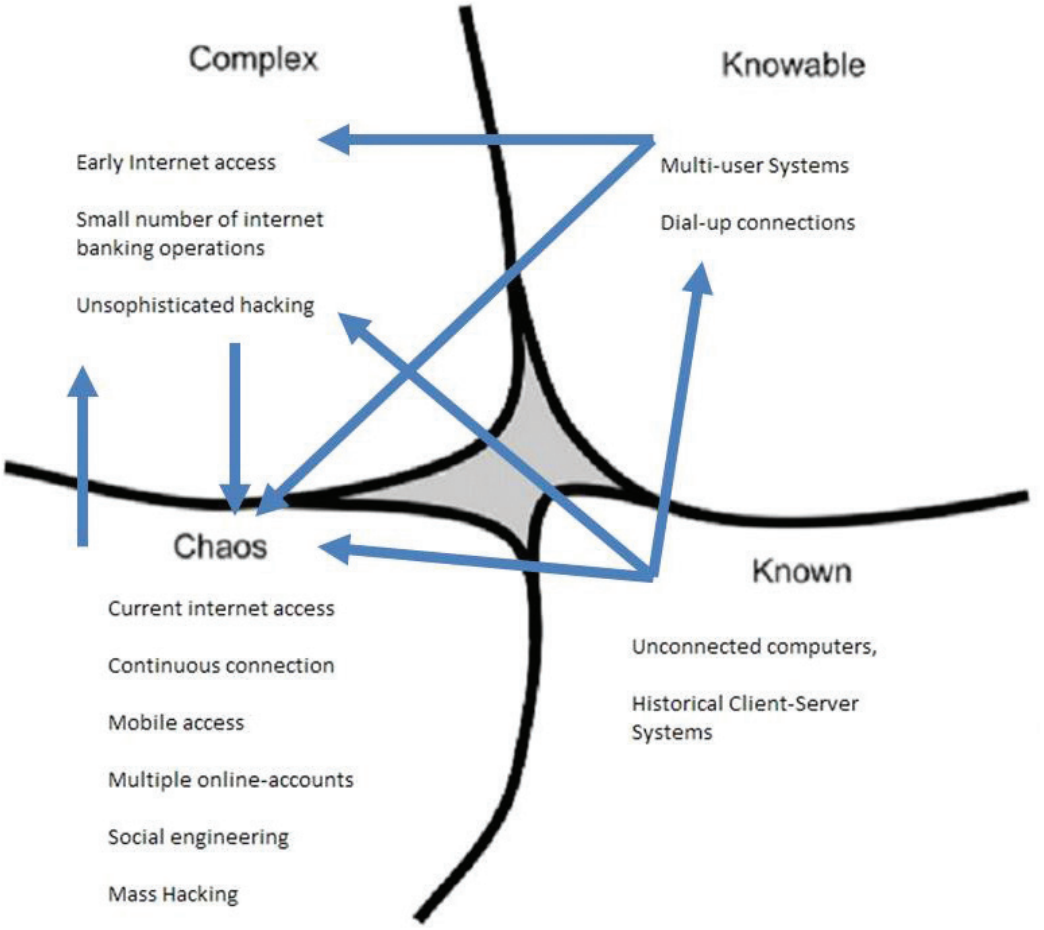
As the framework indicates the issues considered in any concept of system has the perspective of space, time, and connectivity. Here the use of passwords as a tool for providing security in computers and the information systems are provided as an example of issue mapping on Cynefin Framework.

It is known that a link is as strong as its weakest link (Goldratt, 1997) when considering the password based securities which are the "keys to the network kingdom" (Burnett & Kleiman, 2005). Whereas a simple alphanumeric combination was secure enough for the protection of information in the personal computers fifteen years ago, when internet connectivity was rare, today with being online is the blood of daily work life a more rigorous approach to passwords is required. The security issue revolving around passwords can be thought as the polio pandemic (Honan, 2012). Altough it has been a disease found in many civilizations for thousands of years, polio became one of the most dreaded epidemics in the 20th century (Trevelyan, Smallman-Raynor, & Cliff, 2005).

In the course of password use in early systems, direct physical access to the computer of interest had to be accessed directly by the attacker and the password had to guess the password with available personal information about the habits of the system owner or knowledge of that particular system. With the rise of internet the necessity to have access to personal information has changed into access to connectivity time. Using random number generators and dictionary attacks, it became a matter of time to break into the system. While in the early development phases of such attack, methods used required specialized programming techniques and encryption methodology with the rapid diffusion of information and availability of purpose build software any willing party currently has the possession of this capability independent of their level of expertise.

Although it is regarded as an outdated mode of security, established habits and lack of viable alternatives make password usage the default method of security. For example, with 10000 most common passwords representing the passwords of 99.8% of all users (Burnett, 2011) pass the security of an ordinary user's computer in a matter of minutes. Moreover with the current level of connectedness and interdependence of human and information systems the security domain is much more open to manipulation through social engineering attacks, which almost makes all the deliberate systems of security obsolete.

Figure 2: Shifts of issues over ontological domains



As illustrated in Figure 2, issues shift in the ontological domains even before related parties are able to get a comprehensive understanding on the subject let alone develop solutions. One critical aspect of Cynefin framework can be illustrated with the necessity of meta-thinking about the nature of the issues and circumstances, required before diagnosis and solution development. Whereas it would be enough to classify and respond in known domain now that the issues have shifted to Chaotic and Complex domains, it is far from a valid approach.

Conclusion

People make decisions not as a result of consideration and deliberate cognitive processes but as a way of being (Keen & Morton, 1978). The simple and complicated domains represented in the Cynefin framework can be epistemologically classified ordered domains within which a desired output can be determined in advance (Snowden D. J., 2005). Complex and Chaotic domains are in the same sense unordered domains. This means decision makers trading ordered systems or managing the systems in ordered states have the luxury to define goals into the future. Plans that draw the path to achievement of these goals can be made, and through good data capture, analysis can be executed. The unordered systems make determining the output or end-state impossible since the 'relationships between cause and effect are not repetitive except by accident' and the great number of interacting agents and interactions prevent prediction by use of outcome-based models. In that case the right approach would be controlling or manipulating the starting conditions, the containers of the system, significant differences, and the exchanges happening in the system (Eoyang, 2004) to influence the system so that a desirable outcome can be achieved or a failure can be avoided.

Thinking and using right paradigms when approaching issues are critical for the governance of IS security, especially in today's environment where social, business, and cyber are inseparably intertwined. Cynefin framework can in such a time used for sense-making and a foundational framework for decision makers.

References

Ackoff, R. (1974). *Redesigning the Future.* New York: Wiley.

Ajans. (2014, February 25). Retrieved from SonDakika: http://www.sondakika.com/haber/haber-basbakan-devletin-kriptolu-telefonlarini-5712478/

Akerlof, G. (1970). The Market for Lemons: Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics, 84*(3), 488-500.

Alpcan, T., & Başar, T. (2006). An intrusion detection game with limited observations. *12th Int. Sym. on Dynamic Games and Applications.* Sophia Antipolis.

Bloomberg. (2012). *The Price of Cybersecurity.* Bloomberg.

Burnett, M. (2011, 06 20). *10000 Top Passwords*. Retrieved from Xato: https://xato.net/passwords/more-top-worst-passwords/#.UymXeVck-Qs

Burnett, M., & Kleiman, D. (2005). *Perfect Passwords: Selection, Protection, Authentication.* Massachussets: Syngress.

CEN. (2004, March 01). *European Guide to good Practice in Knowledge Management.* Retrieved from European Committee for Standardization: ftp://cenftp1.cenorm.be/PUBLIC/CWAs/e-Europe/KM/CWA14924-01-2004-Mar.pdf

Chang, F. R. (2013, November 5). Studying the 'Wicked Problem' of Cyber Security. *Cyber Security News*, 1-2.

Eoyang, G. H. (2004). Conditions ofr self-organizing in Human Systems. *Futurics, 28*, 10-50.

Epstein, R. A. (1984). In Defense of the Contract At Will. *University of Chicago Law School Chicago Unbound* , 947-984.

Goldratt, E. M. (1997). *Critical Chain.* New York: The North River Press.

Greenwald, G. (2013, June 6). *The NSA Files*. Retrieved from the Guardian: http://www.theguardian.com/world/the-nsa-files

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly, 30*(3), 611-642.

Hasan, H., & Kazlauskas, A. (2009). *Making Sense of IS with the Cynefin Framework.* Hyderabad: Association for Information Systems.

Honan, M. (2012, 11 15). *Why no password is safe from hackers.* Retrieved 04 1, 2014, from Wired Magazine: http://www.wired.com/2012/11/why-no-password-is-safe-from-hackers/

Jones, M. G. (2013). *Asymmetric information games and cyber security PhD Dissertation.* Atlanta: School of Electrical and Computer Engineering Georgia Institute of Technology.

Keen, P. G., & Morton, M. S. (1978). *Decision Support Systems An Organizational Perspective.* New York: Addison-Wesley.

Kellert, S. H. (1993). *In the Wake of Chaos: Unpredictable Order in Dynamical Systems.* Chicago : University of Chicago Press.

Kurtz, C., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal, 42*(3), 462-483.

Murphy, T. J. (2011). A comparison of Cyber Attack Methods. *Journal of Physical Security, 5*(1), 78-82.

Rittel, H., & Webber, M. (1975). Dilemmas in a General Theroy of Planning. *Policy Sciences*(4), 155-169.

Snowden, D. F. (2013). Multi-ontology sense making- a new simplicity in decision making. *Informatics in Primary Health Care, 13*(1), 45-53.

Snowden, D. J. (2005). Multi-ontology senes making: a new semplicity in decision making. *Management Today, 20*, pp. 1-13.

Süskind, P. (1985). *Perfume: The Story of a Murderer.* New York: Alfred A. Knopf.

Trevelyan, B., Smallman-Raynor, M., & Cliff, A. D. (2005). The Spatial Dynamics of Poliomyelitis in the United States: From Epidemic Emergence to Vaccine-Induced Retreat, 1910–1971. *Annals of the Association of American Geographes, 95*(2), 269-293.

USNI. (2010). Cyber Threats to National Security. *Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain* (pp. 1-36). Washington: CACI International Inc.

You, X., & Shiyong, Z. (2003). A kind of network security behavior model based on game. *Proceedings of the Fourth International Conference on Parallel and Distributed Computing* (pp. 950-954). Chengdu: IEEE.