Organizations and Competencies in the Cyber Security landscape

Giacomo Minello, minellogiaocmo@gmail.com

Assignment

A 1-2 page paper submitted by Friday 12 noon of the week of the topic on which you choose to do the paper. Your paper will be 15% of the grade. The assignment for your paper is to choose one of the two topics for the week, and compare and contrast the approaches of the companies who presented in that topic session, describing the differences in their approaches to that topic and why you believe these differences exist (i.e. what caused the differences).

I. Organizations

In organization theory, learning how organizations structure themselves has been proved to be no easy task. Traditionally, the organization is described in terms of an organizational chart but that is an inadequate description of what really takes place inside the organization. However, the organigram should not be rejected, but rather placed in context: it tells us some useful things, even though it hides others. While the organigram does not show informal relationships, it does represent an accurate picture of the division of labor, showing at a glance what positions exist in the organization, how these are grouped into units, and how formal authority flows among them. In order to partially solve this problem organizations usually adopt the use of dotted lines representing a reporting relationship that is weaker than a solid line reporting relationship. This allow to add more flexibility to a chart otherwise too rigid to express the organization as a system that include informal communication. While not being a perfect solution, this helps in unveiling the complexity of the flow of information inside a company.

This is, in my opinion, one of the most important takeaways from the lecture: the importance of mutual adjustment as a coordination mechanism. As we saw in all the case presented during the lecture, there are different ways to organize the structure of the cyber security function inside an organization, each one with its own advantages and disadvantages. Thanks to mutual adjustment, an organization can overcome the disadvantages of a structure, like in the case of the CISO reporting to the CIO. But why an organization is structured in the way it is? Obviously, there is no absolute best way to organize the cyber security function inside a company, otherwise we would empirically see just one structure. So, the questions to ask are: does the company decide its own structure or is the structure an emerging property of the company? And then, why the structure change during time?

There are many factors intrinsic to the organization that influence the structure: age, size, technology, etc. One of the most important is the strategy. It could be argued that the strategy of a company is affected by the company's structure. This is a valid observation and in fact we could consider this two factors, structure and strategy, as codependent. However, for the sake of simplicity this codependency can be reduced to a relation of dependency when we start to consider the external factors that affect the structure of an organization. We can say that the competitive environment usually affects directly the strategy of an organization and then, indirectly, its structure. To be more specific to the cyber security function, the environment is typically unstable, complex, diverse, and hostile. The degree to which an organization is exposed to these characteristics of the environment determine how the environment affect the structure. [1]

It would be interesting to asses how conscious these organization are about the relationship between their structure and their environment. Moreover, I would guess that we could consider the threat landscape and the threat model as an effective description of the environment in which a cyber security unit exists.

So coming back to the first question I would be confident in saying that both are true, the company decide its own structure and that the structure is in part an emerging property of the company. On why the structure change over time there is a simple explanation: it's a reaction to the changes in the environment and to the changes in the intrinsic factor of the organization. However, this is no surprise if we consider that a cyber security function of an organization is in itself an organization, just a smaller one, and if we consider that most of the theories that apply to the organization can be applied to a part of the organization. Another interesting takeaway is that the most common structure among the organizations that we discussed during the lecture is that in which the CISO report to the CIO, as in the cases of Levi Strauss, Novaris and Schindler. My explanation of why this happens is that probably this structure is the most flexible one, optimal in a very dynamic environment and in companies of that size.

II. Competencies

The competencies of an organization are directly related to the skills of the individuals that it is made of and the coordination of such skills. In the case of cyber security, competencies assume a key role in ensuring the security of the organization itself. There is a clear distinction between the structure of an organization, its "DNA", and the organization's competencies, something that we can compare to the "Phenotype" of an organization, opposed to its DNA.

This analogy is effective in describing one of the reasons why organizations with the same structure behave differently and possesses different competencies. This approach to organizational studies is called organizational ecology. The approach of organizational ecology is to apply the evolutive theory to organizations. Assuming that the most important organizational routines are semi-fixed, the way in which an organization can evolve is by changing its competences. In biology, the impossibility for the phenotype to modify the genotype is an assumption of Darwin's theory of evolution.

However, organizations are subject to slightly different rules and we can observe that they behave according to Lamarck's theory of evolution, in which an individual can change its own genotype. While Lamarck's theory has been proven wrong in biology its principles can still be applied to organizations. This model lead to an extremely complex evolutive process. For instance, we can observe the behavior of the NKCS model, a model describing how organizations change their characteristics in order to have more chances of survival[2]. But what can we conclude from this? For sure there is a set of competencies that can be considered a baseline skillset but every organization will have different nuances.

The case of cyber security competencies skillset is particularly interesting when considered in its evolution. The need of cyber security competencies is a relatively recent needs for organization, so according to Lamarck's theory, the adoption of such skills was a change made by the phenotype to its genotype in order to increase its chances of survival in response to a change in the environment (that in organizational ecology is called "ecosystem"). Now, in a complex competitive ecosystem there can be new competencies that a particular organization consider an advantage but this can only be an educated guess. The only way to be sure of such advantage is by analyzing such change a posteriori. The most likely case is that the new skill confirms its usefulness or turns out to be a neutral change (what is effectively an "neutral mutation"). One thing we can be sure of right now is that the skillset needed for competing in the cybersecurity environment changed since its introduction, like in the case of the recently acquired relevance of cyber risk governance, and it will continue to change in response to a complex evolution of the threat landscape.

References

[1] Henry Mintzberg. "The structuring of organizations". In: *Readings in strategic management*. Springer, 1989.

[2] Julian Padget et al. "Sendero: an extended, agent-based implementation of Kauffman's NKCS Model". In: *Journal of Artificial Societies and Social Simulation* 12.4 (2009), pp. 824–844.