Interdisciplinary Description of Complex Systems 16(3-A), 313-319, 2018

THE CYBERSECURITY CAPABILITY ASPECTS OF SMART GOVERNMENT AND INDUSTRY 4.0 PROGRAMMES

Miklós Kiss* and Lajos Muha

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.2
Regular article

Received: 14th February 2018.
Accepted: 31st August 2018.

ABSTRACT

To operate smart cities it is necessary to have proper governance, industry and services ecosystems that can be built upon. The smarter the elements of the system are, the more complex IT infrastructure will be; and these will directly or indirectly have an impact on each other. Last year signified how vulnerable these industry and service systems are in the government and corporate sectors. Significant cyber-attacks such as Wannacry or NotPetya can influence the operations of an organization to a degree that might pose a challenge to governments of cities, countries or even a continent. These campaigns targeted industrial and supply chains. How was survival possible? What competencies were needed to operate our industry in such a harmful environment? In this study we will highlight which competencies are needed for Smart City and Industry 4.0 to successfully implement major projects that benefit the development of smart cities.

KEY WORDS

competencies, IT governance, industry 4.0, smart city, program management

CLASSIFICATION

ACM: K.4, K.6
JEL: A10, C10

*Corresponding author, η: kismkls@gmail.com; –;
H–1428 Budapest, Pf.:31, Hungary

INTRODUCTION – INFORMATION FLOW THAT MAKES YOU SMART

It is not easy to accurately define what a Smart City or Industry 4.0 is, as these are continuously transforming and forming. At the same time, we can find some fixed points with an evolved consensus. The most basic criteria is probably that in respect of both ecosystems sensors and information flow between separate elements occur which enable aligned and closely coherent operation and development of complex systems [1].

The concept of Smart Cities includes and integrates both information and communication technologies and numerous other physical technologies, such as the Internet of Things (IoT), that made possible the optimization and high efficiency of services and city operations [2]. In the field of industry, similar processes are underway at companies, when automation (Industry 1.0) was followed by mass production (Industry 2.0), then computerization (Industry 3.0), and today by organizing actual objects and sensors into networks we have reached Industry 4.0 [3]. IoT, cyber-physical systems and artificial intelligence promoting data interpretation and utilization appear here as well [4].

Several internationally acknowledged companies recognized these aspects of information technology and combined them with their own core competences. Cisco and IBM possess programs, projects and methodologies to promote the integration and connection of these technologies in the modern industrial and urban environments [5, 6].

However, to analyze the issue, it is not enough to apply the technocrat approach alone. One has to take into consideration the complex approach in which the other elements of the ecosystem are also included: people, government, economy, environment, mobility and viability [7, 8], Consequently, when speaking about Smart Cities and Industry 4.0, we need to refer not only to the technology, but we should think about the utilized systems (citizens, enterprises), implementation of missions, operational and strategic governance [9]. It is important to mention that beyond international good practices, domestic regulation was also created: Government Decree 56/2017. (III. 20.) on the modification of certain government decrees related to the definition of *Smart City* and *Smart City methodology*, which among others, highlights the requirements of connection with innovation and strategy [10]. Hungarian Lechner Knowledge Center promotes the improvement of Smart Cities on domestic level [11].

So, we can see that when we want to study smart systems, we also need to bear in mind other elements of the ecosystem (government, enterprises, and organizational abilities). To be able to operate Smart Cities and advanced industrial conformations in the long term, we need to be able to implement these innovations (programs, projects) and make them sustainably operational afterwards.

The issue of cybersecurity is a very important factor in terms of the complex information infrastructure. The higher the complexity of an ecosystems' information network the more vulnerable these systems will be. Therefore, from the moment of planning of these innovations, one has to deal with the projects' cybersecurity matters as well [12]. Availability, confidentiality and integrity are fundaments in which all circumstances have to be secured to sustain stable conditions [13]. The so-called Big Data, originated from sensors and other sources, also represents a major challenge for designers of smart ecosystems [14]. So, in this research, we try to find those organisational competences and features that promote the secure innovation and operation of cities and industrial facilities.

In the following section, we will highlight the cybersecurity challenges of Smart City operators by demonstrating an example case. The third section will introduce competences that may achieve long-term development and projects of a 4th generation enterprise or developed government.

MODERN WAY OF EXTORTION THAT MAY EVEN DISABLE CITIES

In 2016 an interesting incident kept the world and especially the citizens of San Francisco awake. The city's public transportation system was disabled by a ransomware for a long time; a HDDCryptor variant made the data stored on the public transport companies' computers unaccessable [15]. In 2017, another challenge was put to companies utilizing information technology. These two incidents of large-scale impacted both company and government information technology systems.

The WannaCry ransomware campaign occuring in May 2017, spread so fast that the protection utmostly utilised defensive system (SIEM, IPS), operation approach (backup, obsolete systems, ITIL) and human skills (awareness). The reportedly state-sponsored campaign highlighted that an attack of this kind is a potential risk to Smart Cities and industrial facilities connected to a network [16, 17]. The NotPetya campaign following WannaCry pointed out how a targeted campaign can be managed, against government targets. Although there was some collateral damage, the main impact was to a country's information technology infrastructure [18, 19].

These events illustrate the importance of allocating project and operational competences to enterprises investing now in Industry 4.0 innovations. Cities establishing their own Smart City infrastructure also require project and operational competences. What are these competences? This research on organisational competences impacting the success of IT (safety) projects and programmes is trying to determine the answer to this question.

SECURITY CAPABILITY ASPECTS OF SMART PROJECTS

The aforementioned cases highlight that to operate smart ecosystems it is indispensable to have IT systems that enable interconnection and operation of complex systems. For Smart Cities and Industry 4.0 however, beyond technological components competences are required that promote safe operations. Planning and implementation of innovations/projects with respect to IT security is also required. The research mentioned further in the text aims to define these competences, in other words, what are the variables that characterize the enterprise and civil service sector. How do these two segments relate and which components of the main variables have the most significant impact on the complete ecosystem? One further benefit of the research is that we can have a screenshot of the actual situation in relation to both the governmental players and industrial players concerned in the supply chain.

STUDY ON THE FACTORS IMPACTING THE SUCCESS OF SMART CITY PROJECTS

Organization maturity: questions in this group were framed based on the COBIT maturity model, therefore the relation of variables also reflects the sequence (from management to process improvement) [20]. This section of the research points out that the usual maturity level of organizations is typically between maturity level 2 and 3 (this is supported by the lower variance of the responses to these two questions: 0,78 and 0,97). There is stratification between governance and industrial units around maturity level 3 (2,44 and 3,10). This indicates that governance processes are on one hand documented, but there are no real measurements and feedback on the other hand. Generally speaking, maturity of civil service organisations lags behind enterprises. This confirms the need to emphasise competences in Smart City projects.

Logical controls of the organisation: Answers to the questions in this competence group shows there is no significant difference between enterprises and governments. However, it is

clear that enterprises implement more security planning and to risk analysisat project planning which will be required in complex Smart City governance as well [21, 22].

Development demand of organisations: Effort for the qualification of employees is similarly present in both government and enterprise organisations (governments do not reach enterprise levels though). This indicates that besides the operation of complex Industry 4.0 and Smart Cities, resources have to be allocated not only to the qualification of co-workers, but to raise awareness of all stakeholders, especially of the general population (see cybersecurity challenges of technologies mentioned earlier) [23].

Strategy: The greatest difference has been registered in the frequency of regular reviews of the created strategies. While in the field civil service this correction is done every 2-3 years in average (due to reasons traced back to political cycles), private organizations review strategies annually. This implicates the need for restructuring todays' civil service systems of cities of the future (the integration of results of the rapid technological development should be integrated into legislation as quickly as possible) [24].

Efficiency of projects: Investigation of this variable resulted that project management techniques (e.g agile innovation or Scrum methodology) necessary in a dynamically developing city can not really be implemented into todays' civil service. Results are centered around the mean of 3, based on which, at Smart Cities a lot of attention has to be paid to fulfill the social requirements at the highest possible level [25].

The research aimed to prove if variables of the four competence groups have any impact on the *project success*, and to find the significant variables. One single variable was created for the "project group" which contains the characteristics of the five separate variables belonging to four groups. This requirement can be fulfilled by the so-called dimension reduction, that is, by generating a principal component. By generating the principal component, the $n > 5p$ rule is fulfilled, Bartlett's test returns a significant value, KMO value is 0,788, which suggests good suitability. Communality values over 0,5 indicate that the explanatory power of the variables used in the final model is still adequate. In the final model, the principal component explains 57 % of the variance of the other variables which only just confirms the model's validity. With the regression analysis performed with the only variable explaining project success generated this way, we managed to identify the variable components with the highest impact on the dependent variable. Multiple regression analysis was performed by competence groups in each case with the exclusion of non-significant variables (backward elimination method).

Maturity: regression model is $-1{,}851 + 0{,}263 \cdot documentedness + 0{,}358 \cdot innovation$, zero-order collerations of the coefficient table contains the relationship between the independent variable and dependent variable, which shows a weaker than average result (0,394 and 0,492), the models' explanatory power is still adequate: $R^2 = 0{,}302$. In this case, maturity levels of 3 and 5 (documentedness of processes and routine of innovation) have significant impact on the project success, while the regression model did not indicate significant connection in terms of maturity levels 1, 2 and 4. Apparently, it is important to identify and regularly review the processes of these complex smart ecosystems.

Control: $-2{,}612 + 0{,}196 \cdot security\ planning + 0{,}215 \cdot daily\ practice + 0{,}360 \cdot incident\ management$, zero-order correlations indicate average relationship with the independent variable (0,502, 0,458 and 0,587), the model's explanatory power is average: $R^2 = 0{,}471$. Clearly, consideration of security aspects, complying with well-defined rules and well-defined incident management practices have impact on success. Therefore, cyber security incidents will be manageable both for governance and industry.

Development: –2,002 + 0,245·*employee qualification* + 0,376·*structure change*, zero-order data indicate average correlation here also with the project success variable (0,498 and 0,579), the model's explanatory power is still adequate: R^2 = 0,390. Education of co-workers and structure changes aligned with the project have significant impact on the project success of future cities and industrial units. This indicates that government organisations regularly running projects should consider developing a more flexible structure supporting management, and should not disregard competence training of employees and of the population.

Strategy: –1,645 + 0,221·*strategy depth* + 0,378·*strategy review frequency*, based on zero-order data, strategy depth has weak correlation (0,358), while review frequency has medium connection (0,471) with the dependent variable. The model's explanatory power is just acceptable: R^2 = 0,283. Depth of strategies (organisation, IT, IT security) and update regularity of these have impact on the success of delivered projects. Therefore, leaders of those cities and enterprises that do not attend to strategy planning and regular update, will eventually be at a disadvantage compared to organisations that disseminate strategies of appropriate depth and quality.

SUGGESTIONS AND AFTERWORD

Summarizing the identified variables by competence groups (maturity, control, development and strategy) – 5 per group, 3 in the development group – was an important step to get to know the current situation of the civil service and enterprises, which also helps us understand requirements of the Smart Cities and next-generation industry. The comparative investigation pointed out that government organizations lag behind the market players. Enterprises' maturity – especially on level 3 and 4 – is considerable, which is reflected by the effective performance of daily functions and in the quality of performed tasks. Fine-tuned action plans based on measurements enable quick interference so that Smart City and Industry 4.0 innovations can be utilized at the highest possible degree:

- considering the result of the research, that industry organizations have a higher maturity level, their involvement and the best possible utilization of synergies is necessary (see examples from IBM and Cisco),
- security planning should be delivered at the planning phase of complex projects/programs; it is not enough to attach the adequate controls to the programs defining the future retrospectively, as in this case there will be an increasing gap between the real risks and application of regulations,
- it is important to base information security on real incident management procedures (with respect to increasing risks due to new technologies) where the full incident lifecycle is followed.

New technologies mean new risks as well. This research, revealing relevant competences is an assistance for managing these risks of the key projects of future cities and industries.

REFERENCES

[1] Hamblen, M.: *Just what IS a smart city?* https://www.computerworld.com/article/2986403/internet-of-things/just-what-is-a-smart-city.html, accessed 12th February 2018,

[2] Cohen, B.: *The 3 Generations Of Smart Cities.* https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities, accessed 12th February 2018,

[3] –: *Production, organized in networks, or what is "Industry 4.0". In Hungarian.* http://lignomat.hu/HiREK/Halozatba_szervezett_gyartas_avagy_mi_az_az_Ipar_40.html, accessed 12th February 2018,

[4] –: *Industrial Automation.* https://www.lanner-america.com/knowledgebase/industry-4-0, accessed 12th February 2018,
[5] IBM*: IBM builds a smarter planet.* https://www.ibm.com/smarterplanet/us/en, accessed 12th February 2018,
[6] Cisco: *Cities and Communities*. https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities.html, accessed 12th February 2018,
[7] Szendrei, Zs.: *Smart City, the city of the future.* http://www.urb.bme.hu/segedlet/varos1/eloadasok_2014/07B_SMART%20CITY_SZENDREI%20ZSOLT_kivonat.pdf, accessed 12th February 2018,
[8] Giffinger, R.: *Smart cities Ranking of European medium-sized cities. Vienna: Center of Regional Science*. http://www.smart-cities.eu/download/smart_cities_final_report.pdf, pp.10-12, accessed 12th February 2018,
[9] Lados, M.: *Smart cities treatise (IBM).* Hungarian Academy of Sciences, Institute for Regional Studies, West Hungarian Research Department **16**, 2011,
[10] *Government Decree 56/2017. (III. 20.) on the modification of certain government decrees related to the definition of "Smart City" and Smart City methodology.*
[11] –: *Smart City.* http://okosvaros.lechnerkozpont.hu/hu, accessed 12th February 2018,
[12] Lados, M.: *Smart Cities – Smart people.* XVI Actual issues of urban traffic, http://www.ktenet.hu/download.php?edid=1123, accessed 12th February 2018,
[13] Gordon, A.: *CISSP Training Series.* CRC Press, New York, 2015,
[14] Nyikes, Z. and Rajnai, Z.: *The BIG DATA Application to the Hungarian National Digital Infrastructure.* Professional Muster: Academic-professional magazine of the Military National Security Service. Special issue, 74-85, 2015,
[15] Gibbs, S.: *Ransomware attack on San Francisco public transit gives everyone a free ride.* https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware, accessed 12th February 2018,
[16] *WannaCry: Are you safe?* https://www.kaspersky.com/blog/wannacry-ransomware/16518, accessed 12th February 2018,
[17] Gallacher, L. and Morris, H.: *ITIL Foundation Exam Study Guide.* John Wiley & Sons, London, 2012,
[18] Rothwell, J.; Titcomb, J. and McGoogan, C.: *Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down.* http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1, accessed 13th February 2018,
[19] Landry, J.; Izraeli, N.; Shamir, U.; Fenton, C. and Liba, I.: *Dissecting notPetya, SentinelOne whitepaper 2017*. https://go.sentinelone.com/rs/327-MNM-087/images/Dissecting%20NotPetya%20-%20WP.pdf?aliId=21202168, accessed 12th February 2018,
[20] IT Governance Institute*: COBIT 4.1.* IT Governance Institute, Rolling Meadows, 2007,
[21] –: *Act L of 2013 on the electronic information security of state and local government and organizations.*
[22] –: *Minister of Interior Decree on the requirements for technical security, secure information technology devices and products, and security class and level classification defined in the Act L of 2013 on the electronic information security of state and local government and organizations*. 41/2015. (VII. 15.)

[23] Gallacher, L. and Morris, H.: *ITIL Foundation Exam Study Guide*.
John Wiley & Sons, London, 2012,
[24] Kápolnai, A.: *E-business strategy for enterprise senior management*.
Aula, Budapest, 2002,
[25] Szabó, L.: *Project management.*
Pearson Education, Harlow, 2012.