HAL
archives-ouvertes.fr

Understanding the Importance of Proper Incentives for Critical Infrastructures Management – How System Dynamics Can Help

Denis Trček, Jose Gonzalez

▶ To cite this version:

Denis Trček, Jose Gonzalez. Understanding the Importance of Proper Incentives for Critical Infrastructures Management – How System Dynamics Can Help. 1st International Conference on Information Technology in Disaster Risk Reduction (ITDRR), Nov 2016, Sofia, Bulgaria. pp.1-8, 10.1007/978-3-319-68486-4_1 . hal-03213113

HAL Id: hal-03213113
https://hal.inria.fr/hal-03213113

Submitted on 30 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Understanding the Importance of Proper Incentives for Critical Infrastructures Management – How System Dynamics Can Help

Denis Trček[1] and Jose J. Gonzalez[2]

[1] Laboratory of e-media, Faculty of Computer and Information Science, University of Ljubljana, Večna pot 113, 1000 Ljubljana, Slovenia
denis.trcek@fri.uni-lj.si
[2] Centre for Integrated Emergency Management, University of Agder N-4898 Grimstad Norway
josejg@uia.no

Abstract. Computer and information systems are now at the core of numerous critical infrastructures. However, their security management is by far not a trivial issue. Further, these systems, by their very nature, belong to the domain of complex systems, where system dynamics (SD) is an established method, which aims at modelling such systems, their analysis and understanding. Further, on this basis it enables simulation of various policies to properly manage complex systems. More precisely, through understanding of the basic elements of the whole mosaic and their interplay, proper incentives can be tested. And this is important, because proper incentives can lead to the desired patterns of behavior of such systems, which may often be counter-intuitive. Therefore this paper presents a novel approach by using SD for managing critical infrastructures (more precisely the internet) when it comes to security related incentives. Based on already developed archetypes it provides a template model that bridges these conceptual models with concrete models that are suited to particular environments, and enable quantitative simulations.

Keywords: Critical infrastructures, Policies, Management, Modeling and simulation.

1 Introduction

Proper incentives that are implemented through policies or regulation are very vital for complex systems management as they often lead to counterintuitive or even unwanted consequences. History provides many such examples. In 1920, the US government implemented very strict alcohol production, distribution and consumption prohibition legislation. The effects were at least surprising. Strong alcoholic drinks started to flourish (in particular gin), as they were easier to transport and sell secretly than weak alcoholic drinks (for the same effect for consumers). Before this legislation, pubs were almost exclusively visited by men. But when illegal market appeared women often accompanied men at the selling spots – and so they started to consume alcohol, too. But probably the most unwanted effect was that black market became increasingly controlled by the mafia. Consequently, its power increased, and the mafia became and remained a very

strong player due to this source of income even after 1933 when President Roosevelt banned the legislation of alcohol prohibition [1].

This is by far not the only case of an incentive which has resulted in completely unwanted consequences. Some recent incentives that are likely to result in unwanted effects (based on evidence and lessons learnt in the respective field) are those by the US government where flooding-prone areas are declared as safe despite the evidence of the contrary (being stimulated by a wish to picture "normal" conditions in an endangered areas) [2].

Now getting to critical infrastructures, in particular communications – computer and information systems security incidents are a consequence of interplay of numerous inter-related factors. Among those factors human based ones are often at the core of related problems. And proper policies – more precisely, proper incentives – may have a strong impact as to the desired outcomes here as well. One widely known example is the case of ATMs security in the banking sector. When it came to a dispute between a customer and a bank because of a fraud, the burden of proof was put on the banks in the US case, while in Europe, the burden was put on customers. Counterintuitively, the final result was that the overall ATM security was better in the US than in Europe (and all this at lower costs). The core of reasoning was that banks are easier to put appropriate prevention measures in place due to their knowledge and economic power. Put another way, those who should knew better and have more power in their hands should be primarily in charge [3].

Therefore proper incentives are clearly important and they should be carefully studied. As this is easier said than done (one should think only about experimenting with various incentives in real, large scale, environments), appropriate methods that could provide steps into the right direction are much desired. Put another way, to foster aligned incentives it is much desired to have tools for their verification, or at least for playing with associated scenarios to figure out what the unwanted effects of these incentives could be. And this is the main contribution of this paper that is focused on critical infrastructures management, more precisely, cybersecurity. The paper builds on System Dynamics (SD) that has a long and proven track record in various areas of complex systems, including their management. Not only that it enables understanding of complex dynamic systems in a very intuitive way (which is very fine for non-experts), it also enables their modeling and validation (to support with scientific rigor appropriate decision making procedures and management).

This paper presents further steps in the direction of using SD to improve critical infrastructures systems security through aligned incentives. Therefore in the second section the basics related to incentives are given. In the third section the further extension of archetypes is given that results in a template model, which can be adapted to particular cases in a quantitative way. Discussion comes next, being followed by conclusions in the fourth section. The paper is concluded by references.

2 Understanding the Battlefield Landscape

Traditional economics and security relationship was pointed at already years ago in the pioneering papers written by Anderson and Moore [4 - 7]. Summing up the main messages of these works is as follows:

- With current IT technology, attacks are easier than defense. Suppose that a software solution has 1,000 bugs, and for each of those the MTBF is 1,000 hours. Suppose further that a defending user of this software wants to patch it as much as possible and invests 10,000 hours in testing per year. In one year the defender will therefore find (on average) 10 bugs. On the other hand, the attacker can afford only 1,000 hours of testing per year, and will therefore find (on average) only 1 bug. Now one can easily calculate the low odds that this last bug will be one of those 10 ones discovered by the defender.
- Asymmetric information, as applied to ordinary economics by Akerloff, is playing its role also in case of IT solutions [8]. Suppose an experienced vendor offers 10 good security assuring products at 200.- EUR each, while another option are 10 weak security products at 100.- EUR each. Clearly, a vendor can (or is likely able to) tell the good from bad, but buyers cannot. According to Akerloff, users are rational (which is often not the case cases in reality) giving the starting price at 150.- EUR based on the assumption that they are going to get with equally probability a good or a bad product. At this price the seller is motivated to sell only the weak product, so the spiral of negative market selection process is started.
- Network externalities effects stimulate, among others, producers to get on market as soon as possible, which put a pressure on extensive security testing. Thus "get on the market first and do the fixing later" is often a dominant strategy to enable the "get big fast" effect. Further, due to the reinforcing loop of these effects, the winner takes it all situation starts and the landscape becomes more and more uniform. Further, security is often a barrier in usability terms, so even when it is available, the product is configured by default in a rather moderate way. As a consequence, the increasing proportion of systems is becoming susceptible to the same kinds of attacks, so any kind of "epidemics" becomes a natural threat.

To remedy this kind of situation Anderson and Tyler propose avoiding the principle of misaligned incentives, which relate to allocation of security risks. Put simply, those that are most responsible (or in a privileged position) for providing security are usually the least affected by negative consequences. As already mentioned, one typical example where the testing of this claim proved as correct is ATM and credit card frauds.

Based on the above described lessons learned, the following non-technical countermeasures have been proposed:

- Ex ante regulation instead of ex post liability – simply put, involved entities ae liable for their products and services [7].
- Related information disclosure – involved entities should be stimulated to disclose security related information, ranging from found bugs (which is already happening [9]) to aggregated or estimated loss figures (which is yet to be implemented on a

wider scale). This issue is closely related to enabling cyber insurance for taking appropriate precautions that would result in better and more consistent data statistics. An interesting variant of this idea is liability in case of Digital Millennium Copyright Act (DMCA). Here in case of a copyright infringement an internet service provider (IS) is not automatically liable. However, it becomes liable if, upon notification, it does not remove or block the distribution of copyrighted material [7].

- Accreditation and education level requirements – software engineers and programmers should become subject to accreditation requirements and related procedures. It is rather surprising that the essence that runs at the heart of today's critical infrastructures (i.e., software) can be designed and implemented by virtually anyone. Something like this is unimaginable in other important domains like medicine, jurisprudence, and civil engineering, to name a few [10].

There are likely other options for counter-measures – see, e.g., [11, 12]. And to further identify them it helps to ask oneself the following question: "Which are the motivations for people that would stimulate them to act in a way that would improve security of the internet?"

3 System Dynamics and Evaluation of Proper Management Policies

System dynamics (SD) is now an established research and application method that has a proven track record in many areas. As briefly described in [13], system dynamics addresses people, processes, material and information flows by emphasizing the importance of feedback loops. These feedback loops are the major cause for the behavior of (mainly non-linear) dynamic systems.

The modelling starts with a qualitative stage where basic variables are identified and linked accordingly. Through iteration stages the model is improved and the above mentioned causal loops emerge in more and more refined form (consequently, these models are also referred to as causal loop diagrams). As to the links among variables, they have positive polarity if an increase (decrease) of causal variable results in an increase (decrease) of the consecutive variable. But if the output variable is decreased (increased) by an increase (decrease) of the input variable, the polarity is negative.

To obtain models that can be simulated one must transition from causal loop diagrams, where one does not distinguish between different kind of variables, and stock-and-flow models. In the stock-and-flow model version, variables are divided into auxiliary ones and accumulators (also referred to as levels or stocks), where levels play special roles in a system. First, they are the source of inertia. Second, they constitute a kind of primitive memory within the system – an aggregate of past events. Third, they serve as absorbers, and decouple inflows from outflows.

The causal loop diagram is developed provides a holistic view of the system, and enables a better understanding of the basic principles of its functioning. As indicated above such a causal loop model is usually further elaborated to obtain a quantitative

stock-and-flow model. In a stock-and-flow model concrete relationships between variables are established through the introduction of appropriate equations. The model at this stage is ready for calibration based on real data, and use for system simulation and policies derivation.

In order to provide additional insights into incentives issues, and enable appropriate counter-measures that would improve critical communications infrastructure security, appropriate conceptual and template model(s) would be useful. This has been shown to be the case with many other areas addressed by SD like market penetration of a product, infections spreading, and so on.

Now as to conceptual models – for our particular domain two key system archetype models have already been developed [10]. However, archetype models are a special category of causal loop diagrams [14, 15]. They are purely qualitative models with an intention to provide only the basic understanding of the core of a phenomenon at hand. But in order to obtain a quantitative model (that is usually at the top of the agenda) one still needs to fill the gap with so called template models, which identify not only the core variables (factors), but also the related complementary variables, and the nature of the involved variables.

3.1 The Template Model Preliminaries

Now which could be the main motivations of people when it comes, in general, to ensuring security of the internet? Among the main motivation groups are those about avoiding bad reputation (being an unreliable partner, a partner causing damage …), those about avoiding penalties (being charged, being arrested, being disconnected from the internet ...), and those that are about preventing unnecessary or excessive costs (how much to invest in security in order to not to invest too much). This is, of course, not the exhaustive set of possibilities, but it is sufficient to enable derivation of the desired template model.

3.2 The Template Model

In line with the above described reasoning, there are four lines along which the needed SD template model is to be built: The first one is the core of the problem, which is the lifecycle of vulnerabilities and related threats. The second line is the actions line, which is actually in close interplay with the third line, the line of incentives (policies) that are at the core of the analysis. The fourth line is the "final judgment line", i.e., the line that quantifies the success of implemented incentive (policies) in terms of financial gain or loss.

Now the explanation along the horizontal lines follows that sticks with the internal logic of the observed system(s). The vulnerabilities line starts with vulnerabilities production rate. These are vulnerabilities that are a side product of each system design and they remain silent as potential vulnerabilities until they become discovered. Depending on their discovery rate, the appropriate proportion of potential vulnerabilities becomes a recognized fact, i.e., vulnerabilities with an active damage potential. As an active vulnerability is in principle not an isolated one, this active vulnerability typically leads

to additional (cascaded) vulnerabilities. These latter vulnerabilities are usually not immediately recognized; therefore they fill the accumulation of the potential vulnerabilities. The vulnerabilities line ends with the sink of active vulnerabilities that are eliminated due to being fixed or becoming irrelevant (e.g., when the technology is changed).

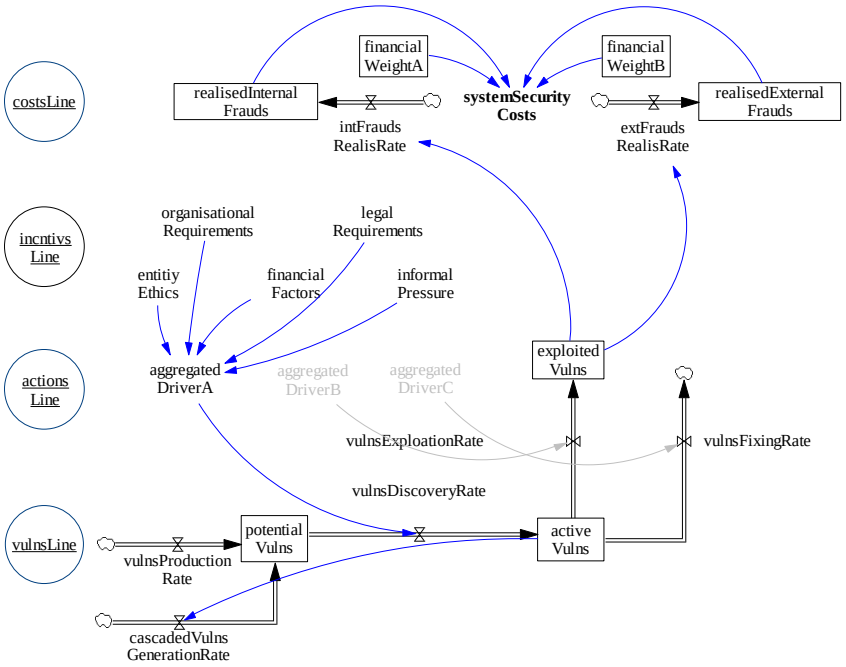

Fig. 1. The template model with the layered factors and their interdependencies

The next line is actions line, where aggregated effects of incentives (from the third, policy line) play the key role. Aggregated drivers are linked to appropriate flows and actually "turn into reality" the dynamics of the observed system (note that for a better clarity only the links for aggregated driver are given). Depending on how successfully we manage the key rates (i.e., the vulnerabilities discovery rate, the vulnerabilities exploitation rate and the vulnerabilities fixing rate) the extent of exploited vulnerabilities is obtained. And using according financial weights the total security cost (that is due to exploits) is obtained. A cautious reader may see that the total security costs could be obtained by taking into account also costs of organizational requirements, informal pressures, and so on (indicated, but not further detailed in the model).

4 Discussion

The above template model per se is still a qualitative one – but with a difference from its archetype counterparts. First, it enables deeper understanding of all variables that

are driving the phenomenon at hand within the community. Second, it serves as a building block that can be turned straightforwardly into a full-blown quantitative model, which can be tested – and tuned accordingly – based on real data. Actually, such template models (although they are referred to as template models here for the first time) are crucial parts of system dynamics arsenal. This arsenal contains not only basic models (like, e.g., the core logistic curve model) but also their more elaborated variants (like, e.g., the Bass Diffusion Model) [16]. And this latter is actually a kind of a template model.

The reason for such step by step approach is rather evident – every model needs to be fine-tuned to a specific case with particular variables. But getting real data to obtain quantified cyber-security models is not a trivial task – on the contrary. So making security measurable is high on the agenda for quite some years. Although the situation is still not an ideal one, it should be stated that some notable advancements have been done in this area, mostly due to MITRE Corp. initiative called Making Security Measurable MITRE Corp. [9].

We anticipate that right at this point template models will provide additional advantage. Their elaboration within the community (as this is normally the case) is expected to result in one or more stable representatives, where it will be clearly visible, which variables (still) need to be collected, what the nature of these variables is, and how they can be tested for consistency. Not to mention that such situation would be already very close to automation of related processes, including testing of incentives.

5 Conclusions

It is known for a long time that cyber security is not just a matter of technical issues, but at least as much a matter of issues that include economics elements and agents' motives. These issues are all subject to incentives, and when properly aligned, these incentives may result in effective (although often counterintuitive) consequences that lead to improved security of targeted systems at lower costs. One typical example is the case of ATM frauds as a result of different incentives in the US and EU – while in the first case the burden of proof was put on banks, in the second case it was put on customers. But surprisingly, US banks had lower frauds number, and the total security costs was lower.

The above instructive case is the main motive behind this paper that is about aligned incentives for improving cyber-security. By using system dynamics we have extended the related artefact models with a template model that fills the gap towards quantitative models, which can be calibrated with real data, so the incentives can be verified accordingly. By doing so proper alignment of incentives is enabled through testing of various policies and their consequences before being implemented in reality.

References

1. Bastable, J., Mason, A., Allan, T.: Great Secrets of History. The Reader's Digest Assoc., London (2012).
2. Horowitz, A.: New Orlean's New Flood Maps: An Outline for Disaster. The New York Times, Opinion Today. (June 1, 2016).
3. Anderson, R.: Security Engineering, John Wiley and Sons, New York (2001).
4. Anderson, R.: Why Information Security is Hard? An Economic Perspective. In: Proc. of the 17th Computer Security Applications Conference, ASAC'01, IEEE (2001).
5. Anderson, R.: The Economics of Information Security, Science 314 (AAA), 610-613 (2006).
6. Anderson R., Information security: Where computer science, economics and psychology meet. Philosophical transactions of the Royal society 367, 2717—2727 (2009).
7. Moore, T.: The Economics of Cybersecurity: Principles and policy options. Int. Journal of Critical Infrastructures Protection 2, 103-117, Elsevier (2010).
8. Akerlof, G.: The Market for Lemons: Qualitative Uncertainty and the Market Mechanism. The Quarterly Journal of Economics 84 (3), 488-500 (1970).
9. MITRE Corp.: Making Security Measurable, https://makingsecuritymeasurable.mitre.org/, last accessed on 6th May 2016.
10. Gonzalez, J.J., Trček, D.: Proper incentives for proper IT security management - A system dynamics approach, HICSS'17, Hawai (2017).
11. Arief, B., Bin Adzmi, M.A., Gross, T.: Understanding Cybersecurity from Its Stakeholders' Perspective. Security and Privacy, IEEE, 15 (1), 71-76 (2015).
12. Arief, B., Bin Adzmi, M.A., Gross, T.: Understanding Cybersecurity from Its Stakeholders' Perspective - Defenses and Victims, Security and Privacy. IEEE, 15 (1), 84-88 (2015).
13. Trček, D., Trobec, R., Pavešič, N., Tasič, J.: Information systems security and human behavior. Behaviour and Information Technology, Taylor and Francis 26 (2), 113-118 (2007).
14. Senge, P.: The Fifth Discipline, Doubleday, New York (1990).
15. Wolstenholme, E.F.: Towards the Definition and Use of a Core Set of Archetypal Structures in System Dynamics. System Dynamics Review 19(7), 7-26 (2003).
16. Sterman, J.: Business Dynamics, McGraw-Hill, New York (2004).