Proper incentives for proper IT security management – A system dynamics approach

Jose J. Gonzalez
Centre for Integrated Emergency Management
University of Agder
josejg@uia.no

Denis Trček
Faculty of Computer and Information Science,
University of Ljubljana
denis.trcek@fri.uni-lj.si

Abstract

It has been known for many years that security failures are caused at least as often by bad incentives as by bad design. However, the regulatory correction of bad incentives is not easy in practice and it is still lacking. In the meantime, system dynamics models of security systems can improve the situation by increasing the awareness that misaligned incentives can backfire as long-term consequences of security failures hit back the principal. We illustrate our argument using system archetypes and concept simulation models revealing the impact of two different security strategies, viz. misaligned incentives (the customer having the burden of proof in case of alleged fraud) vs the bank having the burden of proof. From this we argue that online system dynamics could be used in eGovernment to educate principals and the public. Also, legal measures could become more effective when supported with forensic evidence from simulation models.

1. Introduction

An influential article on the economics of information security states that "security failures is caused at least as often by bad incentives as by bad design" [1, p. 610].

A conspicuous example of misaligned incentives causing bad security originates when the organization that is most responsible (or in a privileged position) for providing system security does not bear the full costs of its failure [1, p. 601ff, 2, p. 105ff]. Such bad practice contradicts the well-known insight from legal theory that liability should rest on the party that can best manage the risk.

Other examples of bad security resulting from perverse incentives involve subtle relations between the parties in the security "battlefield" [1, p. 161-169], such as:

1) Software vulnerabilities, that is, bugs in the software that can be exploited by attackers, are numerous and common. Why? Sloppy coding and insufficient testing could be avoided – but it costs and delays the release of the software.

2) Users are typically quite ignorant about the subtleties of information security whereas software developers and vendors of software know much better about the quality of their products. In such a situation of asymmetric information, software developers prefer to rush to the market – so as to lock customers in – by releasing products lacking sufficient security features that the customer anyhow does not request.

3) Also, since software of high quality with respect to security would cost significantly more than software of poor quality security-ignorant users would not pay more for features that they lack appreciation for. Hence, the market is flooded with cheap software lacking appropriate security. In a seminal paper, Akerlof showed that when buyers have less information – and thus less knowledge – about the quality of products as sellers do, both quality and price suffers [3].

2. Proposed measures

Based on the above lessons learned, non-technical and primarily legal measures are proposed in [2]:

1) Ex ante regulation instead of ex post liability – this kind of action should make involved entities aware in advance that negative consequences may call the involved entities for their liability. In case of software vendors, these would have to provide evidence with the product that it has been subjected to adequate (security testing including) development cycle.

2) Information disclosure – this measure would stimulate involved entities to act accordingly. In case of software producers, shedding the light on a case would "disinfect" it. Further, the community has a right to know, which would be an additional feedback loop to prevent unwanted situations. One such

URI: http://hdl.handle.net/10125/41445
ISBN: 978-0-9981331-0-2

requirement would be a mandated regular disclosure of aggregated loss figures related to on-line banking and payment cards. Similarly, control systems incidents and intrusions should be disclosed as well.

3) Cyber insurance – such a market would be a basis for providing incentives of involved entities to take appropriate precautions through better and consistent data statistics, risk-adjustments premiums, and so on.

4) Indirect intermediary liability – there are reasons that third parties may be held liable for the actions of the involved parties. One such successful example is the case with payment cards frauds in the US. But there also exists an interesting variant of such liability in case of Digital Millennium Copyright Act (DMCA) – if there is a copyright infringement, an internet service provider (IS) is not automatically liable. It becomes liable only, if upon notification, it does not remove or block the distribution of copyrighted material. A similar principle could be adopted for ISPs liability in case of malware infection – upon notification they should assist their customers in malware removal.

5) Accreditation requirements for software engineers. Software now rests at the core of all critical infrastructures, while on the other hand almost anyone can actually be a programmer. This is by far not the case in, e.g., medicine, jurisprudence, mechanical engineering, etc.

In a complex global world it will take a long time until effective measures of legal nature have been deployed and work as intended. Is it possible to assist this process in the meantime, say, by education?

Following we show that a system dynamics model of an archetypal example of misaligned incentives explains the impacts of two different security strategies, viz. one with misaligned incentives (the bank customer having the burden of proof in case of alleged fraud) and another with well-aligned incentives (the bank having the burden of proof). The first strategy led ultimately to major costs to the bank (the principal) in terms of compensating the customers who suffered from fraud and in delayed investments to improve security at much higher cost than the second strategy.

In the last section we conclude that online system dynamics could be used in eGovernment to educate principals and the public about the impacts of misaligned incentives. We argue also that the future legal measures could become more effective when supported with forensic evidence from simulation models.

3. Counter-intuitive impacts of misaligned incentives

Misaligned incentives push the costs of security failures on third parties, but this is not the whole truth. Security systems are complex not only in the sense of being composed of a high number of components (the so-called *combinatorial complexity*). The most challenging part of the security system complexity is the *dynamic complexity*, induced by the propagation of effects over time owing to the interdependencies between the system components. Such propagation of effects results in unexpected, counterintuitive dynamic behavior. In particular, unintended side effects can act as boomerangs that, with a time delay, hit back on the owner of the security defenses who intends to push the costs of bad security to third parties.

Accordingly, awareness of the dynamic complexity of security systems can motivate the owner of security defenses to proactively analyze the long-term costs of boomerang effects from misaligned incentives versus the perceived short-term gains by saving on security and pushing the cost of failures on third parties. Actually, once the long-term perspective enters into the analysis the delayed effects of harming third parties may be seen in a new light as additional boomerang effects to be considered. It is not unreasonable to hope that the rules of the game will tip over as security providers increasingly adopt the stance of analyzing security system solutions as complex dynamic systems. Those providers who adopt the principle that liability should rest on the party that can best manage the risk will hopefully over time be rewarded in terms of customer loyalty and expanding market share. A process of insight and education is needed here.

4. Why system dynamics

In this paper we suggest using system dynamics to assist mitigating the occurrence of bad incentives causing bad information security.

System dynamics (SD) is an established discipline that has a proven application track record in many areas [4-6], including in information security. A core asset of system dynamics modeling is its proven capability to change the mental models of decision makers based on insight on the cause effect relations shaping intended and unintended consequences.

Interestingly, an area where system dynamics has had a strong impact is modeling for litigation and disputes in project management [7-9, 10, p. 170-171]. Hence, the question arises as to whether system dynamics also could clarify causes and responsibilities in terms of post mortem models of disputed cases

regarding misaligned incentives in information security. We suspend discussion of this question for the time being, but we return to the issue in the final section of this paper.

In the next two sections we proceed to analyze a case of misaligned incentives so as to illustrate the power of system dynamics to reveal unintended long-term effects and explain their counterintuitive impacts, in other words to help educate the parties involved in the security domain. In this respect we alert the reader that the emphasis (to be shown below) on the "feedback loops" of the models is of the utmost importance. *A key tenet of system dynamics is that the interplay of the feedback loops shapes the behavior over time of the system.*

The reader who does not have background in system dynamics should read the short introduction in ref. [11], which also can be found online in the homepage of the System Dynamics Society as the entry "What is SD".

5. Understanding the boomerang effects of misaligned incentives

Since we want to introduce the logic of our argument using system dynamics models it pays to choose a case as simple as possible so that the models are themselves simple enough. The simplest case that comes to mind relates to security issues when banks in Europe and the US introduced Automatic Telling Machines (ATMs).

In a survey of fraud against Automatic Telling Machines (ATMs) at the time of their introduction [12], Anderson found that patterns of fraud depended on whether the bank's customer or the bank itself was liable. In the USA, if a customer disputed a transaction, the bank had the burden of proof that the customer was mistaken or lying; this gave the banks a motive to protect their systems properly. But in several European countries (including Britain, Norway and the Netherlands), the customer had the burden of proof: the bank was right unless the customer could prove it wrong – an almost impossible task. The "lucky" banks in these countries became complacent and careless. Eventually, epidemics of fraud demolished their complacency. In contrast, the banks in the USA and other countries having the burden of proof suffered much less fraud. Most remarkably, they spent less money on security than their European counterparts. Thus, better aligned incentives, whereby the defender suffered most if security was bad, turned out to be the best investment for the banks and for the banks' customers as well [1, p. 611, 12].

For the record: After suffering from the bad experience the European banks changed the rules so that the burden of proof no longer was on the customer.

5.1. Qualitative model of ATM security

Consider first the European ATM case. A typical bank acted by setting up the ATM system so that if the customer disputed the transaction, the burden of proof was on the customer. Thus, the bank's intervention is 'Burden of proof on customers', see Figure 1.

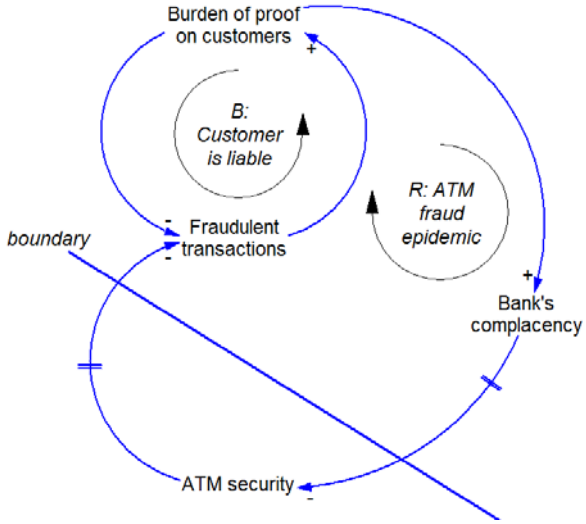

Figure 1 Qualitative model (archetype) for the European ATM case

The intended outcome of the bank's intervention was to reduce the number of fraudulent transactions by the customer (represented by the variable 'Fraudulent transactions'). The influence arrow from 'Burden of proof on customers' to 'Fraudulent transactions' has a minus sign – a negative polarity – expressing that the two variables move in opposite direction. That is, if the burden of proof on customers is increased, the outcome – fraudulent transactions – gets reduced (and vice versa).

The degree to which the intended outcome has been achieved impacts back on the intervention with positive polarity – the more/less fraudulent transactions, the stronger/weaker the bank's intervention is applied. Thus, one has as intended consequence a control strategy, expressed by the balancing feedback loop labelled 'B: Customer is liable'.

The unintended consequence of the bank putting the burden of proof on the customer is an increase in the bank's complacency [1, p. 611] – shown on Figure

1 by the influence arrow from 'Burden of proof in customers' to 'Bank's complacency'. Note that this arrow has positive polarity, expressing that the variables move in the same direction. That is, an increase in the burden of proof exerted on customers increases the bank's complacency, whereas if the bank exerted less pressure on making the customer liable, the bank's complacency would decrease.

In turn, the variable 'Bank's complacency' influences 'ATM security' with negative polarity: an increase in the bank's carelessness decreases the ATM security over time – with some time delay, indicated by ||, as too little is done to analyze the causes of fraud, discover vulnerabilities and exploits, and remedy them. Over time, again with some delay, 'ATM security' influences 'Fraudulent transactions' with negative polarity – expressing that a decrease in 'ATM security' increases the rate of fraudulent transactions – as more and more crooks discover the poor security in the ATMs.

Note that the influence arrow from fraudulent transactions to burden of proof on the customer closes a second feedback loop. Walking along the influence links and considering their polarities it can be recognized that this feedback look is reinforcing (R): if, e.g., the bank increases the burden of proof on customers, the chain of influences along the feedback loop 'R: ATM fraud epidemic', ultimately forces the bank to a further increase of the burden of proof on the customers. The bank's intervention can be characterized as 'barking up the wrong tree', since the intervention is directed to the bank's customers, whereas most of the fraud arises from crooks that exploit the neglected bad ATM security. The straight line in the lower half of Figure 1 serves as reminder that the unintended consequence is 'hidden' beyond a mental boundary of the decision makers in the bank: the unintended consequence is not seen until the resulting ATM fraud epidemic forced a reconsideration of the European bank's strategy.

The causal loop displayed on Figure 1 is an out-of-control problem archetype [13]. The balancing feedback loop 'B: Customer is liable' expresses the intended consequence of the bank's its strategy, viz. to control fraud. The unintended consequence is expressed by the reinforcing feedback loop 'R: ATM fraud epidemic'. Reinforcing feedback loops can act viciously or virtuously, depending on whether they are triggered to increase or decrease unpleasant effects. In this case, the reinforcing feedback loop is vicious indeed. Owing to the banks' refusal to recognize their prominent part in the bad ATM security [12] – expressed symbolically by the boundary line on Figure 1 – and the time delays in the chain of influences, the crooks produced an avalanche of fraud that at long last caused major customer dissatisfaction, loss of reputation and ultimately forced the banks to improve the neglected ATM security – at much higher costs than a well-designed proactive security would have required [1, 12].

Figure 2 adds to the problem archetype of Figure 1 a solution balancing feedback loop (labeled in Figure 2 with 'B: Bank awakes at last'). The bank's new intervention consists in fixing the vulnerabilities in the ATMs in relation to the occurring fraudulent transactions so as to improve the ATM security – all processes that consume considerable time, indicated by the time-delayed influence arrows (marked ||).

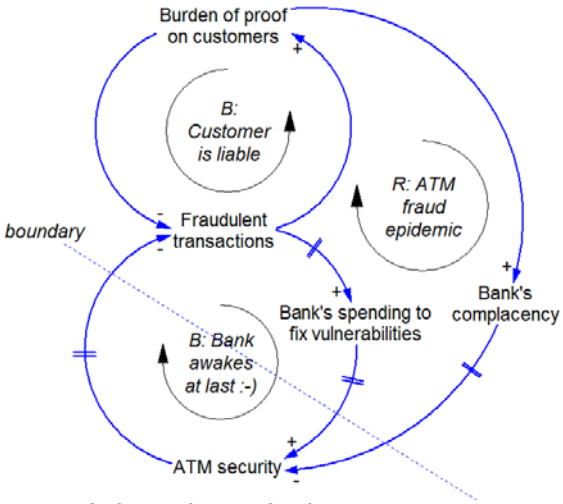

Figure 2 Solution archetype for the European ATM case

Note that the line labeled 'boundary' is shown stippled in Figure 2 – indicating that the mental barrier hiding the unintended consequence from the sight of the decision maker has become 'transparent' upon reflection and understanding. An insightful decision requires consideration of all the relevant aspects of the problem.

In the US ATM case if the customer disputes a ATM transaction the burden of the proof is on the bank. Thus, the bank's intervention is 'Burden of proof on bank' on Figure 3. The intended consequence was to reduce the number of fraudulent transactions (represented by the variable 'Fraudulent transactions') to some acceptable target. The bank assumed the responsibility and spent resources on ATM security as needed (expressed by 'Security spending') [1, 12], which affected fraudulent transactions with negative polarity. To the extent that fraudulent transactions occurred, the burden of proof on the bank was exerted, closing the loop. The intended consequence was controlling, resulting in a balancing feedback loop, labeled 'B: Bank is liable'.

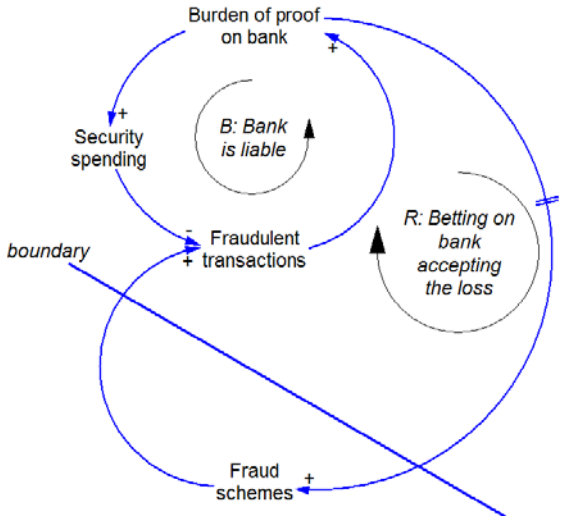

Figure 3 Archetype for the US ATM case

Customers and non-customers know that it is difficult and costly for the bank to prove who did the fraudulent transaction. They know too that the bank will not act if the fraudulent transactions involve small sums of money. Hence, dishonest customers and professional crooks speculated on that, and (with some time delay) they came up with ingenious 'Fraud schemes' (positive polarity), which increased the number of 'Fraudulent transactions' (positive polarity). The unintended outcome was a reinforcing loop ('R: Betting on the bank to accept the loss'). We may assume that this unintended consequence was 'hidden' from the sight of the decision maker – expressed by the straight line labeled 'boundary'. If not completely hidden, we may assume that the bank did not act proactively to mitigate this kind of small fraud until it became sufficiently numerous and costly.

Figure 4 expresses that the typical US bank ultimately developed innovative solutions to stay ahead of the crooks (as expressed by the new balancing solution loop 'B: Improving to beat the crooks').

Also for the US case the causal loop on Figure 3 is an out-of-control problem archetype, following the terminology of Wolstenholme [13]. But the impact of the out-of-control archetypes was quite different for European and American banks.

In the European case the banks did not pay enough attention to the ATM security. As the unintended consequence showed up, with significant time delays (Figure 1), the banks were increasingly facing bad publicity and loss of customers, as well as getting involved in costly court disputes. Sometimes the customers won, making the banks losing face. In the end, the banks had no choice but to acknowledge that the original security solution was bad. They compensated affected customers and had improve security (feedback loop 'B: The bank awakes at last', Figure 2). The security investments were very costly, since the ATM system was not designed with security in mind, and the solution was less good than if the bank had made security a strong priority in the first place [12].

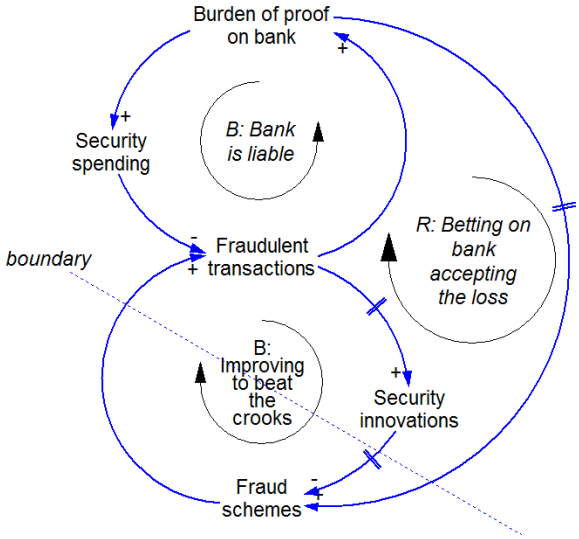

Figure 4 Solution archetype for the US ATM case

In the US case, the banks designed the ATM system with security in mind. Figure 3 shows that ATM security is embedded in the intended outcome feedback loop.

Although advances in fraud schemes forced the US banks to enhance the ATM security, the fact that the banks were security aware and that they were not losing face facilitated a quick reaction and the remedy was less costly than in the European case. This is in accordance with the facts [1, 12].

5.2. Simulation model of ATM security

In the previous section §5.1 we used system archetypes, which are qualitative models, to suggest the causal structure, in terms of balancing and reinforcing feedback loops, to explain the observations about security spending and the fraud patterns when ATMs where taken in use in Europe and the US. However, the analysis of the feedback loops composing the archetypes cannot claim more than to provide plausible explanations. For more convincing evidence it remains to show that a simulation model expressing the feedback loops composing the archetypes is able to render the observed behavior over time for the fraud patterns – the 'reference behavior' for the ATMs in a typical European and a typical US bank.

Regrettably, the information available about the ATM security case in Europe or the US is qualitative and can be expressed in a few statements (p. 3) describing patterns of behavior, rather than providing numerical time series for the key variables of the problem. Given such scarcity of numerical data a 'concept' system dynamics model is a natural choice.

Concept models have traditionally been used by system dynamics practitioners to provide a platform for further exploration of a problem. Concept models – which are simplified and, thus, preliminary – serve as stepping stones towards a more complete understanding of the problem in question by providing insights into the causal structure that could be responsible for the observed over-time behavior [14]. At this stage, all that we require in terms of satisfying the reference behavior is that the simulation reproduces two key observations about *patterns of behavior* (p. 3): 1) that ATMs in some European countries were exposed to an avalanche of fraud while the ATMs in the US were much safer; 2) that the US banks invested less in ATM security while their ATMs nevertheless were more secure than their European counterparts.

We proceed to explain the main features of the concept model of the ATM cases (European and US). The reader interested in the complete details of the models can find the Vensim files in the online proceedings of ref. [15]. Use the free software Vensim PLE for inspection of the model and for simulation. Figure 5 shows features that are common in a system dynamics models for the European and the US ATM case.

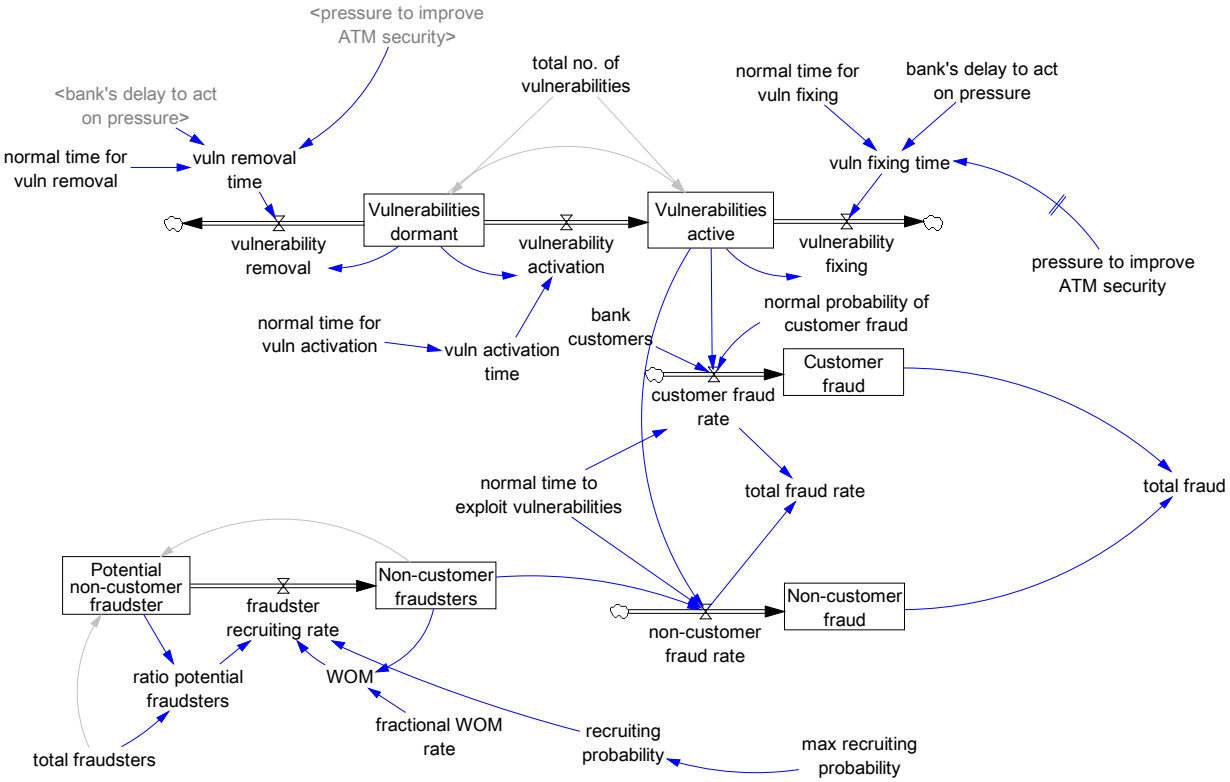

Figure 5 Core structure for a systems dynamics model of the ATM case showing common structures for the European and the US bank

The core model shown on Figure 5 has three structures representing following processes: 1) lifecycle of ATM vulnerabilities; 2) fraud exploiting ATM vulnerabilities; and 3) recruitment of fraudsters.

Lifecycle of ATM vulnerabilities: ATMs have vulnerabilities that can be exploited to commit fraud. Vulnerabilities exist in two states, represented by the stocks 'Vulnerabilities dormant' and 'Vulnerabilities active'. Dormant vulnerabilities have not yet been discovered and, hence, cannot be exploited. By chance or clever schemes, vulnerabilities are discovered and become 'active – that is, exploitable. The flow 'vulnerability activation' in Figure 5 represents the process rendering dormant to active vulnerabilities. Active vulnerabilities are fixed soon after they show up

(flow 'vulnerability fixing'). A proactive posture would in addition imply investment in discovery and removal of as yet unknown dormant vulnerabilities to prevent that they could be discovered and activated by crooks (flow 'vulnerability removal' in Figure 5).

Fraud exploiting ATM vulnerabilities: Figure 5 shows two possible mechanisms for ATM frauds, viz customer and non-customer ("crook") fraud. The model differentiates between frauds committed by bank customers and crooks since the European bank put the burden of proof on customers if they disputed transactions allegedly committed by them. The influence arrows from the stock 'Vulnerabilities active' to the flows 'customer fraud rate' and 'crook fraud rate' express that the fraud rates depend on the extent to which there are active vulnerabilities in the ATMs.

Recruitment of fraudsters: Crooks (non-customer fraudsters) hear about the ATM vulnerabilities by word-of-mouth. The structure with the stocks "Potential non-customer fraudsters" and "Non-customer fraudsters" represents the process of recruitment of fraudsters according to a standard process known as innovation diffusion [6, Ch. 9].

The variable "pressure to improve ATM security" describes how the strategies of European and the US banks (burden of proof on customers vs burden of proof on bank) influenced vulnerability fixing and removal. Accordingly, "pressure to improve ATM security" is affected by different processes depending on the strategy of the banks, as becomes apparent on Figure 6-7.

The pressure to improve ATM security was significantly higher for US banks – who had the burden of proof with regards to fraud claims– than for European banks, who made customers liable and to being with didn't suffer much when fraud was committed.

Figure 6 shows the full system dynamics model for the European ATM case. The core structure that was displayed on Figure 5 is now connected by influence arrows so as to create feedback loops that match the loops contained in the system archetypes Figures 1-2 for the European ATM case.

The variable "proportion of non-customer fraud" (r.h.s. of Figure 6 next to the label "B1: Customer is liable") affects "pressure to improve ATM security". The more fraud was committed by fraudsters, the more the innocent customers of European banks suffered. This resulted in an escalation in angry customer complaints and bad publicity for European banks, ultimately increasing the pressure to improve ATM on European banks.

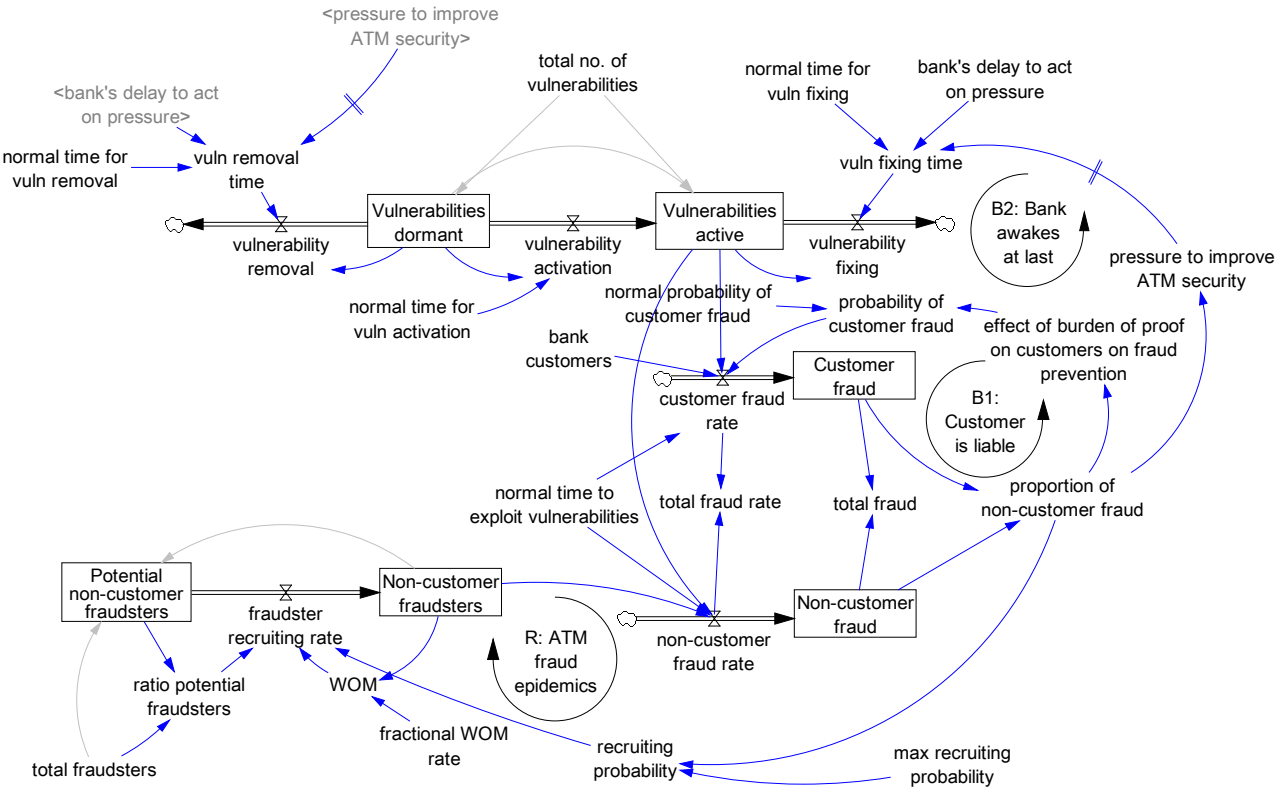

Figure 6 Full concept system dynamics model for the European ATM case

The feedback loops "B1: Customer is liable", "R. ATM fraud epidemics" and "B2: The bank awakes at last" that were already proposed for the European ATM archetype (Figure 2) do occur in Figure 6. Whereas the archetype was only a qualitative model, the full system dynamics model shown on Figure 6 is quantitative and simulatable once all the equations are defined. Hence, it becomes possible to trace the impact of the feedback loops on the behavior over time of the system.

Figure 7 shows the full system dynamics model for the US ATM case. The core structure that was displayed on Figure 5 is now connected by influence arrows so as to create feedback loops that match the loops contained in the system archetypes Figures 3-4 for the US ATM case. Since the burden of proof is on the bank, the US banks assumed a proactive posture regarding ATM security, implying a high value of "pressure to improve ATM security".

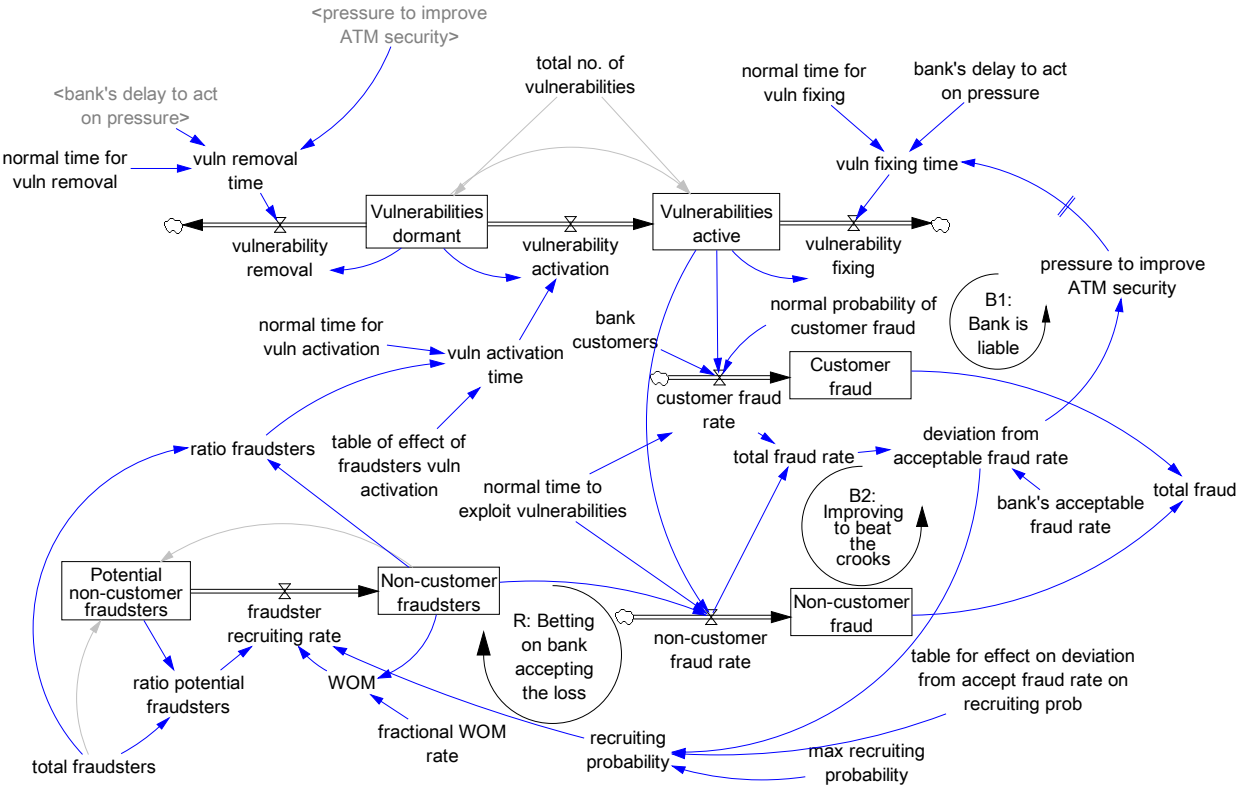

Figure 7 Full concept system dynamics model for the US ATM case

The feedback loops "B1: Bank is liable", "R: "Betting on bank accepting the loss" and "B2: Improving to beat the crooks" that were already proposed for the US ATM archetype (Figure 4) do occur in Figure 7. Again, the figure 7 represents a model that can be enhanced with equations so that it becomes quantitative and simulatable.

The system dynamics models on Figure 6-7 were designed with the simulation software Vensim DSS. Vensim generates equations for the stocks expressing that the value of the stocks accumulates the values of the inflows and de-accumulates the values of the outflows for each time step. The modeler has then to add equations for the remaining variables. The equations for the flows follow standard practice from system dynamics (value of the stock divided by a relevant time parameter). Relations between other variables are expressed using table functions expressing reasonable assumptions (such as that an increasing fraud rate increases the pressure on the bank to fix known, active vulnerabilities).

Some reasonable assumptions have been made as to the total number of vulnerabilities in the ATM as well as to the number of dormant and active vulnerabilities at the start of the simulation. Similarly, reasonable assumptions have been made as to the average times to exploit vulnerabilities, to activate vulnerabilities, etc.

We proceed to discuss the results of the simulation. Figure 8 displays the simulation for the total cumulated fraud committed over time. The curve labeled 1

corresponds to a typical US and curve label 2 a European bank. As in reality, the simulation shows an epidemic of fraud for the European case.

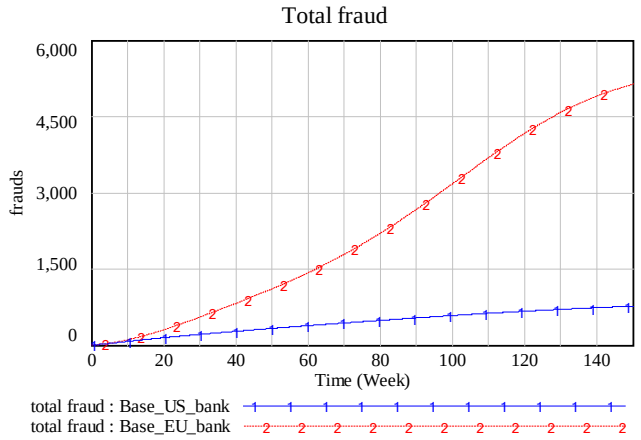

Figure 8 Fraud committed

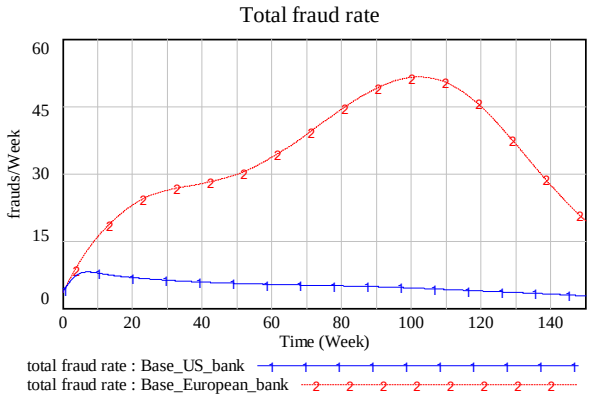

Figure 9 Fraud rate

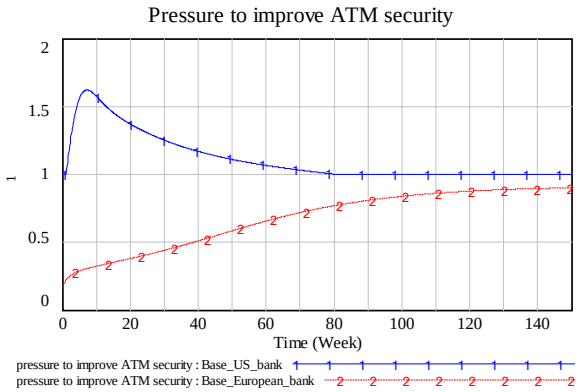

Figure 10 Solution archetype for the US ATM case

Figure 9 displays the fraud rate in units frauds per week. Whereas the fraud rate soon starts decreasing for the US bank, the European bank suffers an increasing fraud rate for a long period of time (for approximately 100 weeks) when it finally starts decreasing as a consequence of the increasing pressure on the bank to improve ATM security (Figure 10).

6. Discussion and concluding remarks

In this paper we illustrated with simple qualitative system dynamics models (the system archetypes Figures 1-4) that misaligned incentives can be doubly misaligned: 1) because third parties, by design, suffer from the resulting externality; and 2) since ultimately the chosen security strategy can hit back the organization that is most responsible (or in a privileged position) for providing system security with a revenge.

Then quantitative system dynamics models were presented. That is, the system dynamics models are "quantitative" in the sense that the simulated time series have patterns of behavior in accordance with the empirical findings of that led to a fraud epidemic in the case of the typical European bank and to much less fraud for the US banks. Hence, the quantitative system dynamics model add evidence that the feedback loops displayed in the system archetypes indeed shape the patterns of fraud that were observed. Here, we remind the reader of the key tenet of system dynamics (see p. 3): the behavior over time is shaped by the feedback loops of the system.

The models do not compute the security costs as such. However, we may assume that the banks ultimately had costs reflecting the amount of fraud committed, that is, in terms for compensating clients. In addition, we may assume that the fact that US banks removed dormant vulnerabilities to a larger extent than European banks will have proven less costly: dormant vulnerabilities that get removed get never exploited and, thus, by this very fact are cheaper than active vulnerabilities which don't disappear until they have been exploited as fraud.

Obviously, it would be preferable if the case chosen for the illustration of the arguments had been better documented in terms of empirical time series for its key factors. Alas, we searched and found nothing. The same applies for other potential cases of interest related to misaligned incentives, their impact on security and their boomerang effects. As in many areas of information security data is detailed data are scarce (or not available). Still we hope that the arguments presented in this paper elicit some curiosity as to the power of system dynamics models to help educate the parties in the "security battlefield". It can be hoped that some organizations come to the insight that it pays to do some modeling to analyze the possible long-term boomerang effects. The cost of developing system

dynamics models is low and the potential gains are high.

As a final remark we comment on the question as to whether system dynamics could help clarify causes and responsibilities in terms of post mortem models of disputed cases regarding misaligned incentives in information security. The question can be reworded as to whether a future introduction of legal measures, similar as those listed in "§2 Proposed measures" should be preceded by an analysis as to factors that should be documented and recorded so as to allow post mortem analysis of responsibilities and liabilities.

In all countries the government ultimately acts as the regulator of last resort and if given good inputs could do so more effectively. In this paper we have shown that concept system dynamics models can provide such "inputs" and do so in a way that can be deployed in digital form for eGovernment. In future work we hope to elicit the interest of experts on system dynamics modeling of project management and of legal disputes on project failures to provide recommendations so as to make system dynamics an assistant and guard for legal measures in information security.

Acknowledgement: Denis Trček thanks the University of Agder for funding his stay as visiting scientist at the Centre for Integrated Emergency Management.

7. References

[1] R. Anderson, and Moore, T., "The Economics of Information Security", Science, 314(5799), pp. 610-613, 2006.

[2] T. Moore, "The Economics of Cybersecurity: Principles and Policy Options", International Journal of Critical Infrastructure Protection, 3(3–4), pp. 103-117, 2010.

[3] G.A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and Market Mechanism", Quarterly Journal of Economics, 84, pp. 488–500, 1970.

[4] J.D.W. Morecroft, Strategic Modelling and System Dynamics: A Feedback Systems Approach, 2nd edn, Wiley, Chichester, 2015.

[5] K. Maani, and R.Y. Cavana, Systems Thinking, System Dynamics: Managing Change and Complexity, Pearson Education, Auckland, New Zealand, 2007.

[6] J.D. Sterman, Business Dynamics : Systems Thinking and Modeling for a Complex World, Irwin/McGraw-Hill, Boston, 2000.

[7] K.G. Cooper, "Naval Ship Production: A Claim Settled and a Framework Built", Interfaces, 10(6), pp. 20-36, 1980.

[8] F. Ackermann, C. Eden, and T. Williams, "Modelling for Litigation: Mixing Qualitative and Quantitative Approaches", Interfaces, 27(2), pp. 48-65, 1997.

[9] K.G. Cooper, and K.S. Reichelt, "Project Changes: Sources, Impacts, Mitigation, Pricing, Litigation, and Excellence", in (G., M.P.W., and Pinto, J.K., eds.): The Wiley Guide to Managing Projects, Hoboken, NJ, USA, pp. 743-772, 2004.

[10] J.M. Lyneis, and D.N. Ford, "System Dynamics Applied to Project Management: A Survey, Assessment, and Directions for Future Research", System Dynamics Review, 23(2/3), pp. 157-189, 2007.

[11] G.P. Richardson, "System Dynamics", in (S. Gass, and C. Harris, eds.): Encyclopedia of Operations Research and Management Science, Kluwer Academic Publishers, Dordrecht, the Netherlands, pp. 1519-1522, 2011.

[12] R.J. Anderson, "Why Cryptosystems Fail", Proceedings of the First ACM Conference on Computer and Communications Security, 1993, pp. 215-227.

[13] E.F. Wolstenholme, "Towards the Definition and Use of a Core Set of Archetypal Structures in System Dynamics", System Dynamics Review, 19(7), pp. 7-26, 2003.

[14] G.P. Richardson, "Concept Models in Group Model Building", System Dynamics Review, 29(1), pp. 42-55, 2013.

[15] J.J. Gonzalez, and K. Lenchik, "The Economics of Cybersecurity: Boomerang Effects from Misaligned Incentives", 34th International Conference of the System Dynamics Society, 2016