A system dynamics case study of resilient response to IP theft from a cyber- attack

Sepúlveda Estay, Daniel Alberto; Khan, Omera

Published in:
Proceedings of the 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)

Link to article, DOI:
10.1109/IEEM.2017.8290101

Publication date:
2017

Document Version
Peer reviewed version

A system dynamics case study of resilient response to IP theft from a cyber-attack

D.A.Sepulveda[1], O.Q. Khan[2]
[1]Department of Management Engineering, Technical University of Denmark, Kongens Lyngby, Denmark
[2]Department of Business and Management, Aalborg University Copenhagen, Denmark
(dasep@dtu.dk)

Abstract - **Undesirable changes in supply chain physical operations derived from disruptions in the transmission or storage of digital information are reported daily despite the Information Technology (IT) protection available. Once a disruption materializes, the company losses will depend on the coherence and swiftness of the supply chain response (resilience). However, current resilience frameworks are qualitative, do not address evolution over time as a relevant aspect, and thus do not provide indications on how to design a resilient response. This paper contributes to closing this gap by developing a system dynamics model from an actual case of resilient response after a cyber-attack. Both case-specific and generic structures are extracted from the case data analysis, and a reaction mechanism is proposed that results in the observed behavior. The identification of these structures should eventually aid decision makers in the process of designing a resilient supply chain response.**

Keywords - Resilience, Cyber-risk, System Dynamics

I. INTRODUCTION

There has been an undisputed increase in the use of Information Technology (IT) in supply chains [1]. This trend is likely to continue as IT enables supply chains to respond to market pressures for efficient operation and customer collaboration during product and service delivery. However, the complex digital network that has resulted has created new sources of risk, mainly related to unintended system flaws that make user error more likely, and results in both internal and external risks [2]. Internal risks are derived from vulnerabilities in the connections between system components that result in risk of failure even if all parts of the supply chain work as expected, and external risks are derived from unauthorized agents exploiting these vulnerabilities for their own benefit.

Intellectual property (IP) is an example of a particular organizational asset which has increased its exposure to theft through the use of IT for its transfer, storage, and development coordination. IP is a central driver for innovation, business growth and competitiveness, potentially constituting as much as 80 percent of a single company's value [3]. Additionally, the Sarbanes Oxley regulation, enforced after the Enron and Worldcom scandals, has imposed accounting rules that result in a greater required detail in the reporting of IP valuation. This has transformed IP from being an internal strategic factor, to being a public financial dimension [4]. Literature informs that the most advanced economies are those with the greatest cyber-related IP losses, theft that accounted for as much of the US$ 200 billion cybercrime losses during 2013 [5].

Traditionally, IP took the form of people inside the organization, with direct knowledge and access to R&D resources, who misappropriated prototypes or documentation, physical or digital. This restricted the potential suspects in cases of IP theft, and it was usually an action targeted to specific documents or technology. The digitalization of IP information transfer and storage has opened the field to IP thieves in any location, allowing for either targeted or opportunistic attacks [6], and allowing attackers to operate in relative anonymity. The pool of suspects is thus far greater, and can include competitors, hackers that do this for money or fun, or even nation-states.

Resilience frameworks have addressed the way a supply chain responds over time to disruption events. Sheffi and Rice [7] described the extent of the consequences derived from a supply chain disruption as derived from the depth and duration of a negative evolution of performance resulting from the disruption, in what they named the "disruption curve". This curve implied that an improved response to disruption would consist of both a shorter and a shallower disruption in performance.

Despite being only qualitative, this approach contrasts to other supply chain resilience frameworks that identify resources and strategies, but do not address the measurement of the evolution of performance [8][9][10].

These resilience frameworks appear to be ill-suited for the challenges presented by cyber-risks in complex supply networks: by focusing on the expected resulting states and pre-existing resources required for a resilient response, the capabilities required to activate, drive and control the response have been comparatively overlooked.

Additionally, the case study method, despite being a very valuable tool for inductively extracting non-structured data about the response to disruptions, lacks a focus on the evolution of this response over time.

Literature has therefore mentioned the potential for complementarity of the case study method with other methods, such as system dynamics [11].

Derived from these gaps, this paper contributes by analyzing a specific case of IP theft resulting from a cyber-attack and looking into some of the concrete organizational structures that drive the resilient response of the organization to this theft. This process results in a dynamic model, and a categorization and sensibility analysis of this structure on the resulting performance

evolution over time. Second, in the process of building this dynamic model starting from the case study description of the IP theft, this paper aims to outline a structured method for "translating" case studies into dynamic response structures that can be quantified and modeled.

The structure of this paper is as follows: section II will describe the methodology; section III will describe the results; section IV will discuss and highlight implications of the results, and describe the limitations of the method, and section V will outline the conclusions and areas of future work.

II. METHODOLOGY

This paper uses the system dynamics (SD) framework to develop a dynamic model representation of a case study. This complementarity is particularly well suited for cases where there is little or no historic information, and where the evolution of performance is a relevant subject of study.

SD is a framework for the representation of systems that change over time by using a network of variables in relationships of circular causality; network composed of fundamentally two types of variables, stocks (accumulations) and flows either flowing into or out of these accumulations. By virtue of different timescales or the specific problem under question, it is sometimes convenient to represent some of these stocks or flows either as constants, or auxiliary variables (instantaneously changing).

The visible state for such a system is therefore completely represented by the values of the stocks in the system and all changes in these stocks is what can be understood as the system's "behavior". These conditions have two very relevant consequences: 1) By virtue of this networked representation, all the behaviors of a system are the direct result of its own structure, in what is termed the "endogenous" view of behavior in SD and 2) any system that changes over time in any interesting way, has at least one feedback loop (the basic circular causality unit) in its structure.

Despite being Forrester [12] who started what can be called the "MIT school" of thought in SD modeling, this paper will use the method outlined by [13], and proposes the following steps: problem articulation, formulation of a dynamic hypothesis, formulation of a dynamic model, testing, and policy design and evaluation.

The problem description and boundaries are obtained from documentation and interviews about the specific case study, and the data that can be extracted from these documents is "translated" into a causal loop diagram and a system dynamics model that is eventually simulated.

III. RESULTS

A. Case description

ABC Industries is a producer of hardware with 60.000 employees and a 12.2 percent operating margin. Six months before a product launch a federal agency informed ABC of a cyber-breach. The effect of this breach was the loss of IP data for 15 out of the 30 product lines. These lines were expected to contribute 25 percent of the company's total revenue for the next 5 years.

The stolen information allowed a hacker to exploit previously undiscovered design flaws, implant malicious code into these product lines, allow competitors to market a similar product earlier undercutting ABC on price.

ABC's reaction had three phases: Incident triage, Impact management and business recovery.

During the incident triage phase ABC brought in the necessary resources to assess the initial damage and prepare the organization for potential consequences of this attack. First, a team of managers and research scientists was formed to oversee the efforts to minimize the effects of this attack. This had negative effect on productivity. Second, an external cyber-security company was hired to investigate the leak, and patch the system to future similar attacks. Third, a law firm was hired to lay out the potential legal ramifications of the breach. Fourth, a public relations (PR) firm was hired to start preparing the commercial ramifications of this breach.

During the impact management phase ABC Industries changed the use of existing resources and processes. Product launch was accelerated by two months, creating a need for additional research personnel and overstretching the capacities of existing research personnel, decreasing productivity. Also, product shipments were suspended while an upgrade was developed for the products as a result of the stolen IP. Important contracts were lost probably as a result of both a decreased perception of product safety in the customers, and by the delayed shipment of existing orders. Contract losses were expected to account for 5 -10% of the projected revenues for the company.

During the recovery phase, ABC industries made structural changes as a result of the cyber-attack. First, it performed an inventory of all its IP, instituted an IP protection program, and upgraded its security infrastructure. Fig.1 shows an evolution of these actions.

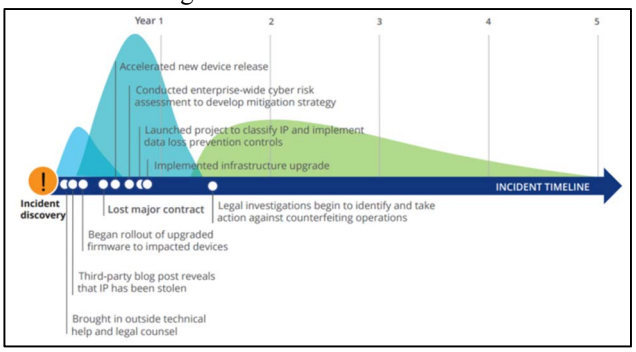

Fig. 1. Action timeline for ABC Industries disruption [6]

As a result of the cyber-attack, ABC industries reported additional costs of US$ 3.2 billion over 5 years. Despite their sales level returning to normal levels after

one year, the total recovery time was of five years. The following figure shows the evolution of the Sales and Profit levels with respect to the expected sales and profit levels, and is in essence the reference mode a dynamic model would seek to reproduce and explain.

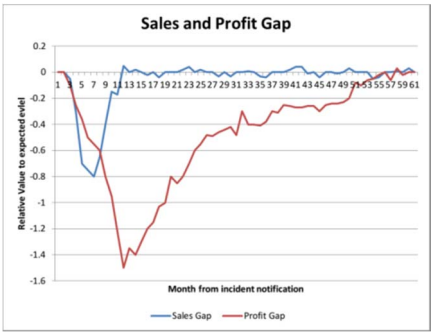

Fig. 2. Evolution of relative sales and profit levels during disruption

B. Model Development

From the case description, a series of circular causality feedback loop "types" can be identified (See Fig.3).

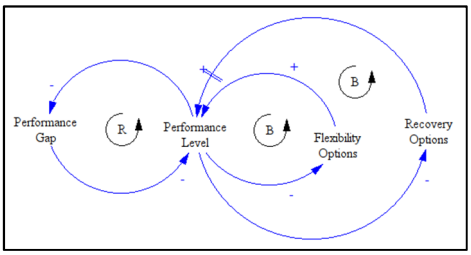

Fig. 3. Generic feedback loop types present during a resilient response

A first type corresponds to those feedback loops that form vicious circles with respect to the declining performance levels. An example of this is the loss of contracts derived from the IP theft: the more contracts or sales are lost, creates an even lower sales level increasing the sales gap and the profit gap.

A second type of feedback loops, are the "flexibility options" that the company uses to manage resources in the short term. The case mentions mainly management and R&D personnel as the internal resources involved, and PR, cyber-security consultants and legal counsel as external resources. The type two feedback loops can be further subdivided into either 1) a redistribution of internal resources (as in the short term there has been limited time to increase these resources), or the hiring of external resources, available quickly, but at additional cost, such as the case of the public relations firm, the cyber-security company and the Law consultant. Both of these options have an effect on the performance, through a decrease in the IP generation productivity, and through the increase in operation costs, respectively.

A third type of feedback loops are those that the company uses to manage the long-term actions, which we have denominated the recovery options. Examples of this include the hiring of additional R&D personnel that was hired for the generation of additional IP. These have effects on costs and are the last ones to be maintained until the company reaches the expected operation level. Figure 3 shows a causal loop diagram (CLD) representing these generic feedback loop types.

The specific loops identified in the description are shown in Table 1.

Table. 1. Feedback loops identified in description

Loop Number	Loop Type	Loop Number	Loop Name
1	Reinforcing	R1	IP Rules
2	Reinforcing	R2	PR to the rescue
1	Balancing	B1	Marketing Stabilizer
2	Balancing	B2	IP Expiration
3	Balancing	B3	Marketing Costs
4	Balancing	B4	Hacker Attacks
5	Balancing	B5	Trust issues
6	Balancing	B6	Productivoty Loss
7	Balancing	B7	Security Costs
8	Balancing	B8	Legal Bundle
9	Balancing	B9	Legal cousel
10	Balancing	B10	Legal costs
11	Balancing	B11	PR Costs
12	Balancing	B12	Leak containment

These Feedback loops represent the circular causality structures present in the case description, connecting relevant variables as seen in Fig.4.

In order to start building a dynamic model derived a first approach considers only the basic loops that create the base behavior, as shown in Fig. 5. The interaction of these loops tells a story of how a resilient behavior comes about without a disruption.

R1, reinforcing loop 1, "IP Rules" feedback loop. This is the main mechanism through which a company based in exclusive IP develops its business. Exclusive IP generates a Demand which is translated into Actual Sales and Actual Profit levels, which are partially invested into the development of more Exclusive IP, expanding the business

R1, reinforcing loop 1, "IP Rules" feedback loop. This is the main mechanism through which a company based in exclusive IP develops its business. Exclusive IP generates a Demand which is translated into Actual Sales and Actual Profit levels, which are partially invested into the development of more Exclusive IP, expanding the business

B1, balancing loop 1, "Marketing stabilizer" feedback loop. This captures the main mechanism ABC Industries uses to counteract differences in demand. Since the development of IP is a long, uncertain process, which is then reflected as exclusive products to the market, the way in which demand fluctuations are counteracted are through changes in the sales strategy through the use of marketing instruments, creating a loop that does not let the Sales Gap to increase endlessly.

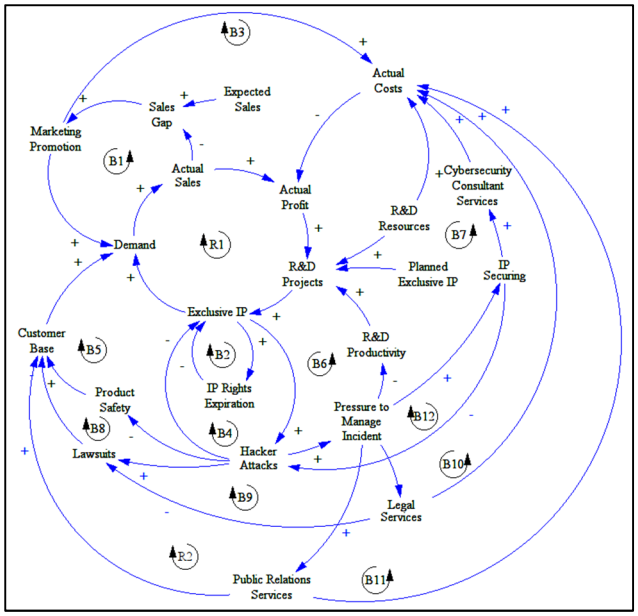

Fig. 4. Feedback Loops present in the case description

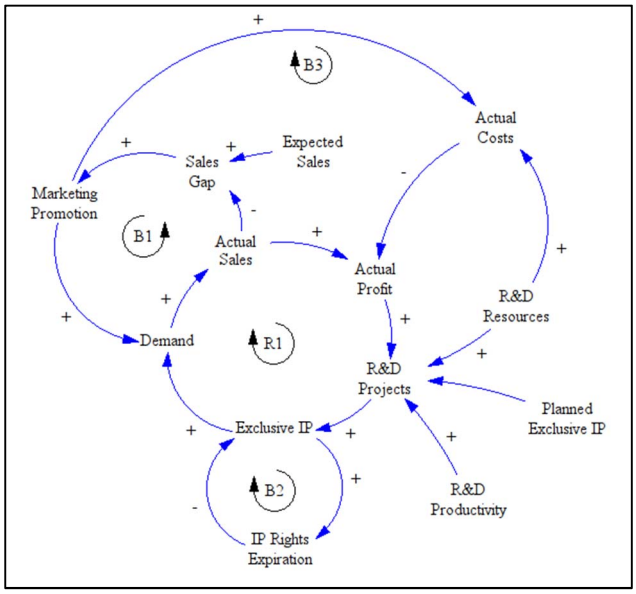

Fig. 5. Basic Feedback Loops present in the case description

B2, balancing loop 2, "IP expiration" feedback loop. This captures the process of IP expiration, resulting from the limited time for which an IP is exclusive to the company that created it.

B3, balancing loop 3, "Marketing Costs" feedback loop. This captures additional marketing costs, which limits the amount of marketing possible as it affects the profit level with a direct consequence in the number of R&D projects that can be started.

The resulting Dynamic model considering these base loops is shown in Fig. 6. The loops correspond to those in the CLD in Fig. 5.

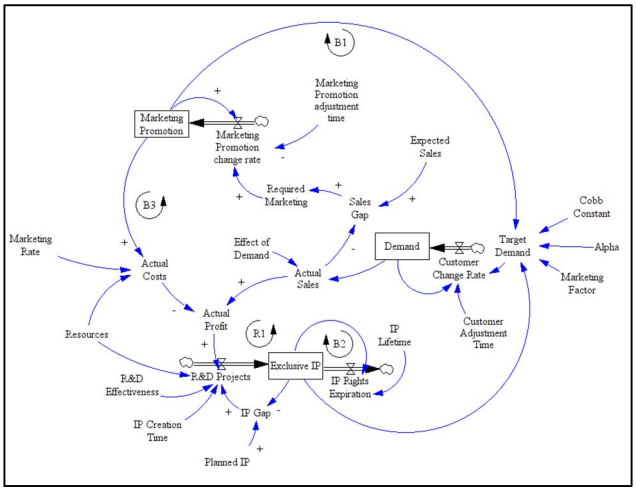

Fig. 6. Stock-and-flow model for the basic model

IV. DISCUSSION

A dynamic model can be validated in a variety of ways, as it has been documented by Senge and Forrester [14].

In this case, the base model was tested from equilibrium for an initial disruption in the level of Exclusive IP stock, and different levels of some of its exogenous variables, i.e., marketing feedback, customer adjustment time and marketing contract times. The resulting Sales Gap for this sensitivity analysis is shown in the following graphs.

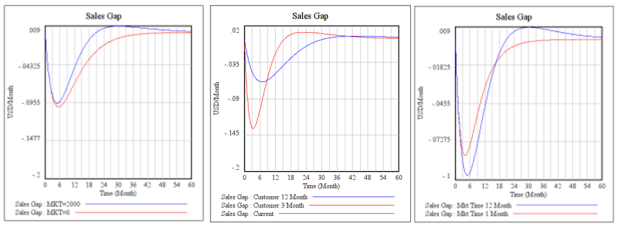

Fig. 4. Basic Feedback Loops present in the case description

Marketing contract time had extreme values of 1 and 12 months, customer adjustment time had variations from 3 to 12 months, and the Marketing Rate had a range of 0 to 2000.

The evolution over time of the sales gap resembles the behavior mode indicated during the case description in Fig. 2. Given the negative feedback loops present a slight over shoot is seen in all cases for one of the extreme values, and the sales gap recovers the desired level after close to 18 months

Despite only considering the feedback loops in Fig.5 from all the ones present in the case description, this basic model points the way forward for broadening and deepening the dynamic representation of the case study. The additional feedback loops should be introduced sequentially, testing how the model behavior is affected by each addition.

This process also illustrates a possible path from Case study to Dynamic Model, summarized as the iterative process of extracting the mental models present in the data, and creating maps of circular causality that drive processes over time: identify the actions from the case, identify the perceived causality of those actions and the variables that are affected in the process. Then by differentiating those variables that are slow to change from those that change quickly, the stock and flow diagram can be attempted.

The data gathering process for this paper revealed two interesting shortcomings with respect to the information available in a case study: 1) the descriptions imply causality without exploring it explicitly. It follows that the information contained in the way in which agents in the system assume the system works, is not gathered 2) There is an idealized process described as a unification of different data sources, obscuring a very important source of unexplained behavior in systems, this being the misalignment between mental models of agents acting in the same system. The contradictions should not be discarded, but rather compared and accounted for, as these might very probably have some influence in "unexplained" system behaviors.

V. CONCLUSION

By developing of a dynamic model based on a specific case study about the resilient response to a cyber-attack, this paper has shown the process of such an approach for representing cross-disciplinary processes that occur when an organization has to manage disruptions. Additionally it has put forward an initial approach for understanding the structure in an organization behind a resilient behavior.

Reaction design will involve the identification of these and other structures, obtaining adequate values for it governing exogenous variables; a crucial activity that will need to be internalized by organizations.

The suitability of undertaking a medium to long-term timeframe analysis of the problems related to the effects of cyber risks in operations, as well as the limited information available about past events of resilient response to cyber-attacks, make SD an attractive tool since it is a methodology less concerned with reproducing past behavior, focusing rather on the structures underlying the observed behavior, through the identification and explicit representation of the mental and formal models present in the organization.

The effect of considering a long-term view, beyond the immediate short term operational pressures, both allows for designing a response that minimizes the overall cost of a disruption, and identifies incentive structures that promote this response.

REFERENCES

[1] G. C. Stevens and M. Johnson, "Integrating the Supply Chain … 25 years on," International Journal of Physical Distribution & Logistics Management, vol. 46, no. 1, pp. 19–42, Aug. 2016.

[2] N. G. Leveson, Safeware: system safety and computers: Boston, Mass.: Addison-Wesley, 2001.

[3] "News Releases," Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC. [Online]. Available: http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/. [Accessed: 31-May-2017].

[4] N. Kossovsky, B. Brandegee, and J. C. Giordan, "Using the market to determine IP's fair market value," Research-Technology Management, vol. 47, no. 3, pp. 33–42.

[5] "Net Losses: Estimating the Global Cost of Cybercrime," Global Initiative, 25-Jan-2017. [Online]. Available: http://globalinitiative.net/documents/net-losses-estimating-the-global-cost-of-cybercrime/. [Accessed: 01-Jun-2017].

[6] J. Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," DU Press. [Online]. Available: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html. [Accessed: 01-Jun-2017].

[7] Y. Sheffi and J. B. Rice, "A Supply Chain View of the Resilient Enterprise," MIT Sloan Management Review. [Online]. Available: http://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/. [Accessed: 01-Jun-2017].

[8] M. Christopher and H. Peck, "Building the Resilient Supply Chain," The International Journal of Logistics Management, vol. 15, no. 2, pp. 1–14, 2004.

[9] C. W. Craighead, J. Blackhurst, M. J. Rungtusanatham, and R. B. Handfield, "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities," Decision Sciences, vol. 38, no. 1, pp. 131–156, 2007.

[10] J. Blackhurst, K. S. Dunn, and C. W. Craighead, "An Empirically Derived Framework of Global Supply Resiliency," Journal of Business Logistics, vol. 32, no. 4, pp. 374–391, 2011.

[11] G. Papachristos, "Case study and system dynamics research: Complementarities, pluralism and evolutionary theory development," 30th International Conference of the System Dynamics Society., vol. 112, 2012.

[12] J. W. Forrester, Industrial dynamics. Cambridge, MA: Pegasus, 1961.

[13] J. D. Sterman, Business dynamics: systems thinking and modeling for a complex world. Boston: McGraw-Hill/Irwin, 2000.

[14] J. W. Forrester and P. M. Senge, Tests for building confidence in system dynamics models. Cambridge, MA: System Dynamics Group, Sloan School of Management, Massachusetts Institute of Technology, 1978.