C.W. Axelrod, Int. J. of Design & Nature and Ecodynamics. Vol. 10, No. 4 (2015) 289–299

ADDRESSING SUPPLY-CHAIN COMPLEXITY USING CLOSED-LOOP SIMULATION-BASED EXERCISES

C.W. AXELROD
Delta Risk LLC, USA.

ABSTRACT

From news reports about companies attempting to reduce the impact of compromised supply chains, due to natural disasters, accidents or targeted attacks, or trying to avoid specific products or ingredients banned on moral grounds, it is apparent that many organizations have only rudimentary knowledge of the provenance of software, hardware, and other supplied items. Reasons for this situation include the difficulty and effort required to:

- build and maintain complete and accurate databases;
- obtain information on subcontractors down to the required level of detail;
- review, monitor and test products to ensure that they are genuine;
- encourage eradication of deficiencies, weaknesses, and vulnerabilities;
- ensure that changes are identified, reported, analyzed, and addressed;
- identify commonalities and common points of failure;
- introduce resiliency, redundancy, and backup within the supply chain;
- develop methods to simulate infrastructures, transactions, etc.; and
- bring together competitors to collaborate in exercising various scenarios.

Thus, the question arises as to how to resolve these issues in an accurate, efficient, and cost-effective manner. Answering this question is our goal.

Supply-chain models are generally substantially more intricate than the model developed for the US equities marketplace. However, the same approach works for developing and operating any complex industry-wide and sector-wide systems with many participants who want to keep proprietary information confidential but need to share information to facilitate a rich exercise experience for learning, training, and testing a variety of realistic scenarios. This paper describes a process for implementing such simulation-based exercises.

Keywords: closed-loop tabletop exercises, commonalities, complexity, complicatedness, counterfeiting, resiliency, supply chain, tampering, transaction-level simulation models, vendor management.

1 INTRODUCTION

Prior to the industrial revolution, supply chains consisted of local suppliers providing limited ingredients to artisans, such as flour to bakers, leather to cobblers, iron to blacksmiths, etc. Over time, products and services became more sophisticated, requiring harder-to-come-by components from larger specialty producers, who benefited from economies of scale. At that time, supply-chain vendors and outsourcing partners were usually well known to customer organizations. Suppliers were mostly domestic, if not local. In these circumstances, they could be audited on-site, with little or no advanced notice. However, suppliers commonly imported raw materials, such as spices, and intermediate products, such as fabrics, from distant lands. This made for additional risk since early forms of transportation, such as sail ships, were often hazardous and, as a result, schedules were uncertain.

Today, supply chains are commonly distributed globally with suppliers thousands of miles from their customers. Also, many components incorporate elaborate software systems and intricate electronic components, which may have been designed in one country, manufactured in another, and assembled in yet a third. As a result, the management of modern supply chains has become increasingly difficult, requiring ever more highly skilled resources. In this paper, we discuss the issues and suggest ways in which many of the problems can be resolved, or at least mitigated.

ISSN: 1755-7437 (paper format), ISSN: 1755-7445 (online), http://www.witpress.com/journals
DOI: 10.2495/DNE-V10-N4-289-299

2 SIMPLICITY, COMPLICATEDNESS, AND COMPLEXITY

The first question to be addressed here is about the very nature of complex systems, from which we can determine if indeed supply chains can be considered to be complex or merely complicated. The differences among simple, complicated, and complex systems have been discussed extensively in the literature, as in [1–8].

The consensus seems to be that complicated systems are aggregates of many components that must operate together in planned, structured, and predetermined ways. Complex systems, on the other hand, are held to be adaptive in response to continual change and uncertainty. This implies that complicated systems are deterministic, whereas complex systems are probabilistic in nature.

We can see distinctions among simple, complicated, and complex systems in Table 1. For example, complicated systems are synergistic, that is, as simpler systems are combined into more complicated systems, the latter may well exhibit capabilities that are greater than the sum of the capabilities of the individual parts. This is similar to what system engineers call 'systems of systems'.

Complex systems, on the other hand, are fraught with uncertainty and cannot be managed in the same way as are complicated systems. They need much more flexible controls and the ability to

Table 1: Definitions, descriptions, characteristics, and examples of simple, complicated, and complex systems.

	Nature of system		
Attributes	Simple	Complicated	Complex
Definition [1]	Systems for which the chances of success are high and easily predicted	Systems that follow patterns and about which accurate predictions can be made	Systems where interactions and consequences are difficult to determine
Description [2]	May require some basic technique and terminology, but then have high assurance of success	Not just an assembly of simple components Nature is related to scale Requires coordination and specialists	Cannot be reduced to complicated problems Requirements based on local conditions, interdependencies, and ability to adapt to change Ambiguous and uncertain
Characteristics [3]	Can be replicated easily Expertise not required Products standardized Consistent results	Assurance of success from prior experience Expertise needed Some commonalities Results certain	No assurance of success Expertise not sufficient Each project unique Outcome uncertain
Examples [3,4]	Following a recipe	Sending a rocket to the moon Building a highway Building an air-traffic control center	Raising a child Managing traffic congestion Directing air traffic

respond quickly to unanticipated events or changes. To some extent, one can consider complex systems to be complicated systems that have been subjected to perturbing random events, so that their formerly stable operation becomes volatile.

3 ARE SUPPLY CHAINS COMPLICATED OR COMPLEX?

When it comes to modern supply chains, they are seem to be increasingly hard to manage, although researchers, such as Brody [9], claim that certain technologies, for example, 3-D printing, will result in simpler relationships between customer organizations and local suppliers, with fewer interdependencies. However, there are many economic factors, such as the availability of skilled labor, cheap raw materials, and efficient transportation, as well as environmental restrictions, which limit the attractiveness of local sourcing.

There seems to be agreement that most modern supply chains are not simple. The issue is whether they are complicated, that is, they can be planned, managed, and controlled, or whether they are complex, that is, they are dominated by uncertainty and the need to adapt quickly to changing circumstances.

From the business perspective, senior executives' want to control supply chains completely, which suggests that they see modern supply chains as merely complicated, not complex. Unfortunately, organizations cannot escape uncertainties experienced through their supply chains as suppliers are dispersed globally among countries with varying cultures, infrastructures, legal systems, and weather patterns, and vulnerability to earthquakes, volcanoes, floods, fires, tsunamis, etc. Therefore, we must accept that many supply chains are indeed complex and we must do our best to mitigate risks that such systems experience.

4 REASONS FOR SUPPLY-CHAIN COMPLEXITY

Deshpande [10] gives five reasons why supply chains are complex. He asserts that a large number of variables, which he calls 'numerousness', makes for complex supply chains. However, complicated systems also have many variables, so that numerousness alone cannot define complex systems. Then, there is 'variety', which refers to variables' distribution patterns, such as seasonal demand. Again, if such distributions are known, then such a supply chain is complicated rather than complex. However, if the distributions show high variability, then systems should be viewed as complex. He claims that 'interconnections' also determine whether systems are complex. On the other hand, however many interactions there might be among parameters, the system remains complicated as long as the interconnections are well defined and stable over time. If there is variability or uncertainty with respect to interconnections, then systems are considered complex.

'Opacity' means that the 'exact nature of (a) relationship' may not be known with certainty. This is a core characteristic of supply-chain complexity. Opacity is often the main reason why companies get into trouble when there are catastrophic events, such as earthquakes or tsunamis, or when governments outlaw certain materials, such as 'blood diamonds' and North Korean gold.

A major recommendation of this paper is to address opacity through anonymous information sharing facilitated by tabletop exercises incorporating simulation models.

'Dynamic effects' relate to small perturbations that are magnified as they propagate throughout supply chains, in the so-called 'bull whip' effect. This supports the idea that supply chains are complex as, for example, when there is a 'lack of information on the true nature of product demand'.

When opacity and dynamic effects are combined, you have the worst of both worlds with respect to supply-chain complexity. For example, relatively small events, not reported to customer organizations quickly enough, may continue to grow until their effects are so great that they severely disrupt business-as-usual and become newspaper headlines.

5 BUILDING VENDOR MANAGEMENT DATABASES

The main antidote to complexity is timely, accurate, and sufficient information. For supply chains, this translates into gathering, analyzing, and acting upon information obtained directly from suppliers or garnered from other parties. For many organizations, the oversight of suppliers is handled by their vendor management departments in concert with internal or outside lawyers. When operating as they should, the vendor management and the legal departments are responsible for collecting data from both internal and external sources on all suppliers dealing with the organization. It is common to use pro-forma surveys for gathering such information. Each vendor is asked to complete the survey in order to obtain the information needed to approve or turn down the vendor. In some cases, the level of detail may vary depending upon the criticality of the supplier to the customer organization. These questionnaires typically consist of dozens of pages of questions, usually with 'yes', 'no', and 'not applicable' responses to facilitate scoring. The analysts may weight the answers with respect to importance, and the resulting score is the weighted sum or weighted average of the aggregated scores. If the total of the weighted scores falls below a particular 'hurdle' number, the vendor may be rejected outright or might be asked for further details related to their initial responses. For example, if a vendor responds that they have a set of security policies, they may be asked to supply evidence in the form of the policies or an audited review that has evaluated the policies and confirmed their existence and appropriateness. The additional information augments the data already collected and all the information goes into a more rigorous evaluation. A process of this type has been formalized in, for example, the Santa Fe Group's Shared Assessment Program (SAP) described in [11], details of which can be reviewed by the reader at http://santa-fe-group.com/capabilities/shared-assessments/. The SAP program grew out of a project originated by the BITS division of the Financial Services Roundtable, which represents major US financial institutions [12].

In many cases, organizations send out vendor surveys annually, or more frequently if the vendor is very critical to the customer organization or if something happens that impacts the products and services being supplied and received. Timing and periodicity, level of detail of information requested, and the like will vary depending upon the criticality of the vendor to the business or as a result of known significant changes in vendors' circumstances, due to, for example, mergers and acquisitions, changes in physical and financial health, business strategies, and the like. If a vendor is important enough to the business, an on-site review might be warranted. If a vendor supplying a European or US organization and/or its subsidiaries works out of Asia, say, it will probably be more cost-effective to employ a trusted local auditing firm for on-site reviews and to report findings back, rather than transporting internal staff to a distant site.

Whichever approach is selected, and wherever critical vendors are located, the main result of all these data gathering effort is a vendor management database containing financial and operational details for each supplier. Also, when non-public personal information, such as data about customer organizations' own or their business partners' customers or employees, is collected and used by service providers, then a whole series of laws and regulations kick in, depending on the location of suppliers and customers. In some cases, countries in which the customer organizations are located determine which legal and regulatory requirements must be applied, even if the supplier is located in a different country. The database serves as a repository of vendor information which informs managers about such details as the date of the prior review, previous scores, and the like, making for much improved supply-chain risk management.

Table 2: Vendor management database actions.

Category	Periodicity	Type of data	Actions
Vendor	Annual Semi-annual On-demand Triggered	Financial Operational Physical and information security Information security Legal and regulatory Locations and jurisdictions Business continuity/disaster recovery	Accept/reject vendor Request additional information Request audit review reports Request security review reports Obtain any certifications Request on-site visit(s) by company or third party
Process	Continuous	Efficiency Effectiveness Accuracy Risk Resiliency	Monitor process to ensure that is in proper working condition Perform third-party reviews Re-evaluate scope of data and risk criteria when bad situations arise
Events	Random	Natural disasters Political situations Local fires, floods, etc. Business events, e.g. takeovers, mergers, relocations Bankruptcies Other business cessation reasons	Assess impact of event Review contingency plans Determine short/long-term options Select appropriate response Initiate business continuity plans Initiate disaster/recovery plans Look for other suppliers/customers

Another mechanism that needs to be in place is a notification process through which the database can be updated and, more importantly, it can be determined whether an audit or business review should be initiated. Unless an effective change notification process is in place, it is very likely that the customer organization will not hear about significant changes in suppliers' financial, organizational, managerial, and operational situations until an adverse event occurs, a change of location is made, or a supplier engages a new subcontractor or outsources certain activities, which brings changes to the fore.

We show, in Table 2, data that need to be collected, monitored, and received as notifications from vendors, vendor-management processes, and material events. We also indicate actions that need to be taken in order to ensure that supply-chain events can be properly managed.

6 VENDOR AND SUBCONTRACTOR DATA COLLECTION

While it is relatively straightforward, though not easy, to obtain survey information from direct suppliers, since they are motivated to remain as suppliers, it has been found to be much more difficult to obtain information about suppliers' subcontractors and vendors. This is in part because companies often view information about their suppliers to be confidential and proprietary. For example, when surveyed about the sources of meat in their products, companies that did respond (several did not) gave the following reasons for not supplying the requested information [13]:

"...we do not normally discuss our sourcing strategies"
"(We do not) provide (vendor) names ... as this is proprietary"
"We don't disclose supplier names for competitive reasons"
"We do not disclose any vendor or supplier information..."

Although it is likely that companies are more willing to disclose supplier information on a confidential basis, where it will not be made public, than to the press, they are still very reluctant to reveal such information even on a confidential and anonymous basis. Also, it is often difficult to convince subcontractors that there is value to them in providing requested information.

A survey conducted on behalf of the US financial services industry, described in greater detail in [14], found that, while many institutions were willing to describe their vendor-management processes and procedures, far fewer responded when it came to actually listing all their suppliers. This appeared to be due to firms' not having readily accessible databases that could have provided such a list. Ironically, many organizations put together such lists as part of their Y2K data-collection efforts, but following Y2K they generally failed to keep these lists up to date. Also, particularly in large organizations, this type of information is scattered across many divisions and departments and does not always exist in a central repository. Even when these lists were developed and maintained, they seldom, if ever, contained information about subcontractors and vendors to suppliers.

Given such a response, one can anticipate considerable resistance from direct suppliers if they were asked to list subcontractors and second-level suppliers. And yet a complete picture is not attainable unless everyone agrees to participate and share information. As discussed later, responses might be better if companies were able to submit information in an anonymous, yet authenticated, manner.

7 TAMPERING AND COUNTERFEITING

In some industries, such as the pharmaceuticals industry, fake products are a huge issue. With physical products, in particular, there are a number of ways to identify the genuine article. However, it is very difficult to know whether there has been some form of tampering of software. There are usually no traces left when software is copied, as would be the case with physical theft. On the other hand, there exist methods to ensure that software cannot be accessed or copied, preserving the original asset and preventing tampering or theft.

Furthermore, extremely complicated equipment, comprising myriads of integrated computer chips that are designed and fabricated using specialized software, can be tampered with at the design, development, manufacturing, and testing phases as well as during maintenance.

Knowledge of the provenance of software and equipment, achieved by tracing through each step in the supply chain, can go a long way towards determining whether specific products should be suspected of having been subjected to tampering or counterfeiting. However, in many situations there is no substitute for full laboratory testing.

8 CHECKING FOR DEFICIENCIES

It is incumbent upon vendors and subcontractors to check their products for software vulnerabilities and weaknesses, as well as for mechanical deficiencies. However, it is up to customer organizations to perform due-diligence reviews to assure themselves that proper care has been applied to the assurance of third-party products and services. One means of achieving this is by incorporating one's own organization's standards, processes, and procedures into contracts with third parties. A particularly strongly worded contract for the acquisition of third-party software was developed by Pelgrin *et al.* [15] in the SANS Application Security Procurement Language document.

When a large customer has relatively small suppliers, that is, suppliers provide the bulk of their output to one particular customer organization, the latter will normally have significant leverage over such suppliers. Under these circumstances, customer organizations can often dictate strong terms in service or product contracts and ensure that they will be permitted to monitor compliance with those terms and conditions. Similarly, large suppliers are able to have customers sign purchase agreements that significantly reduce supplier liability. This balance of power is discussed by Axelrod [16]. However, for the majority of supplier–customer relationships, organizations can neither get agreement on such stringent terms nor can they effectively enforce requests to be informed immediately when adverse events occur. The following section suggests an approach to alleviate this issue.

9 CHANGE NOTIFICATIONS

One of the greatest challenges in supply-chain management is ensuring notification when material changes take place within a particular supply chain. Many suppliers are understandably concerned about revealing proprietary information that might give competitors an edge or bring law suits down upon them. Consequently, they are often reluctant to provide information about incidents that might lead to delays, compromises, or cessation of supply.

Because of this reluctance, we need some method of reducing risks of suppliers making critical information about incidents available to customers on a timely basis, so that the latter can take necessary actions. One suggested means of achieving this sharing of crucial information is for all entities in the supply chain to provide information to a central monitoring body, which then reports significant events to customers. However, if preferred, incident reports can be sent to a trusted third party for distribution to various interested parties, including customers, suppliers, regulators, law enforcement, government agencies (such as emergency and disaster recovery services), and the public at large. The template for such an information-sharing system, in which identities of submitters can remain anonymous and content can be scrubbed to de-identify any attributable information, already exists in the form of industry ISACs (Information Sharing and Analysis Centres). The role of ISACs includes making sure that information comes from authentic sources and adding intelligence obtained from other sources, as shown in Fig. 1.

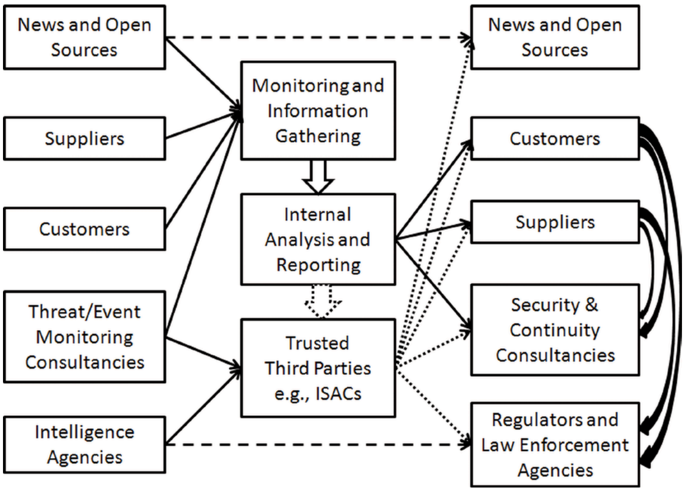
News and Open Sources
Suppliers
Customers
Threat/Event Monitoring Consultancies
Intelligence Agencies
Monitoring and Information Gathering
Internal Analysis and Reporting
Trusted Third Parties e.g., ISACs
News and Open Sources
Customers
Suppliers
Security & Continuity Consultancies
Regulators and Law Enforcement Agencies

Figure 1: Supply-chain information gathering, analysis, and reporting.

Of course, suppliers and customers need to be identified if action is required by business partners, regulators, law enforcement, and even the military. Protocols need to be developed for such situations. A key success factor is a measure of protection so that, for example, proprietary information is not leaked to the public and parties involved have time to prepare a response.

This flowchart can be used as the basis of a computer simulation model, to represent how one might obtain data and report them for complex supply chains, and thereby enable the various entities to respond and resolve issues resulting from incidents. In this manner, the simulation model becomes the basis for closed-loop transaction-level tabletop exercises, as discussed below.

10 COMMON POINTS OF FAILURE

Modern economic systems demand the most efficient production and distribution methods as companies compete on a global scale. This approach favors the trend towards large-scale suppliers and distributors in order to achieve requisite economies of scale. However, this move to fewer and larger entities, along with the just-in-time inventory philosophy to reduce inventory levels and their respective costs, results in more common points of failure, as described by Axelrod [17]. For example, huge manufacturers, such as Foxconn, build electronics equipment for many retail brand names, and suppliers of specialized components provide their products to many different manufacturers and retailers, such as automobile makers.

11 RESILIENCY VERSUS ECONOMICS

As mentioned above, there is often a possible tradeoff between supply-chain resiliency and costs. The former can be achieved by using a bigger number of suppliers and carrying larger inventories, as described in [17]. However, the pendulum is swinging in the other direction. That being the case, the means of risk mitigation is to have a store of data that can be used in preparation for incidents and in real-time when incidents occur. Because these data are difficult and expensive to come by, and, once they have been acquired, require deep understanding and constant updating, the only feasible approaches for handling such vast and rapidly changing data are the use of big-data analytics and computer simulation models, accompanied by frequent reviews and tests to ensure that all the information is current. We will not be addressing the big-data analytical methods in this paper. Suffice to say that the resulting computer simulation will be much superior if relationships among entities, transactions, and events have been established through a combination of analytical results and subject-matter expertise.

12 SIMULATION MODELS AND EXERCISES

There are a variety of ways in which supply-chain simulation can be approached. The choices are among emphasizing infrastructure or transactions, restricting the model to specific marketplaces or expanding it for broad coverage, determining the level of detail, choosing between open-loop or closed-loop models, combining in-person players and virtual players, and the like. Decisions as to the structure and functionality of the model depend mostly on the purpose of the model as well as the cost and difficulty of constructing and operating it. As the DECIDE-FS® model for financial services demonstrated, attaining an accurate, realistic model can be a multi-million-dollar effort extending over many years.

A supply-chain model, even if limited to a single industry, such as automakers or the pharmaceutical industry, is even more complex than that of a single industry, such as financial services, and so it can be expected to be significantly more costly and difficult to build a good representation of supply chains as cooperation among participants will likely be less. Nevertheless, the pay-back can be huge.

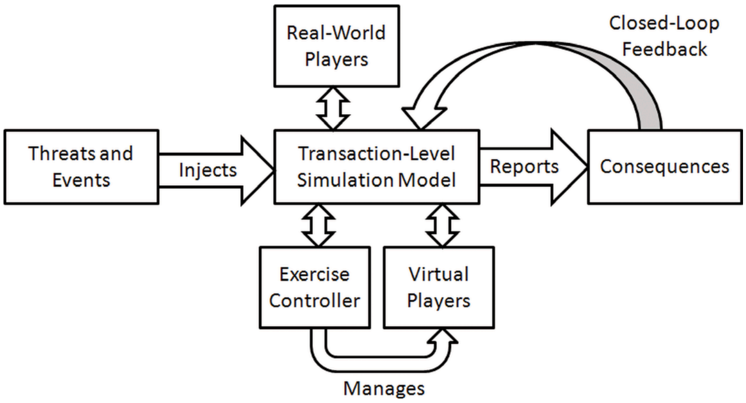

Figure 2: Closed-loop exercise using transaction-level simulation model.

Figure 2 illustrates the structure of a closed-loop transaction-level simulation model and how it fits within an exercise environment. This particular diagram shows a combination of real-world and virtual players, which has been successfully used in several tabletop exercises for the US securities industry. More detailed descriptions of such exercises, as they relate to financial services and supply chains are given in Axelrod and Schmidt [18] and Axelrod [19] respectively. The characteristic to note is the closed-loop feedback arrow, by means of which lessons learned within and between exercises are fed back into the model to serve to improve future exercises. A surprising number of other forms of exercise do not have this type of feedback so that each effort is essentially based on little or no past experience from prior exercises.

13 CRITICAL SUCCESS FACTORS

In addition to getting the model right, to be effective, exercises must not only be well coordinated but they should also exhibit the following properties:

- The right mix of organizations, representing each of the player groups, should participate in exercises, either on-site or remotely.
- Specific individuals from each organization should be carefully selected with subject-matter experts and decision-makers at hand throughout exercises.
- Those running exercises should be very familiar with both the operation of simulation models and how to conduct such exercises.
- Exercises should take place periodically, e.g. twice a year, or when a particular event or situation arises, e.g. the possibility of a pandemic.

14 CONCLUSIONS

Supply chains are becoming increasingly complex and costly to manage, if indeed they can be fully managed. Major incidents have far-reaching effects on the ability of supply chains to operate in a well-controlled manner, and many organizations have neither the tools nor the management support to engage in expensive model building and exercises. Furthermore, sharing accurate, timely information is needed to understand weaknesses in supply chains and to establish greater resiliency of products and services.

Since interdependencies within supply chains are becoming more complex as new countries climb the industrialization ladder, the need for effective tools, greater communication, and more collaboration among business partners and competitors is becoming ever-more crucial. Whereas it would be ideal if supply chains could be simplified, they seem to be heading in the other direction, so that it is incumbent upon us to develop means of dealing with such complexities in order to manage and control supply chains which are increasingly critical to continued economic progress.

REFERENCES

[1] Lelong, A., Complicated systems vs. complex systems, *Global Supply Chain News*, Global Supply Chain Group, December 2013.

[2] Glouberman, S. & Zimmerman, B., Complicated and complex systems: what would successful reform of medicare look like? *Discussion Paper No. 8,* Commission on the Future of Health Care in Canada, July 2002.

[3] Allen, W., Complicated or complex – knowing the difference is important, *Sparks for Change*, available at http://learningforsustainability.net/sparksforchange/complicated-or-complex-knowing-the-difference-is-important-for-the-management-of-adaptive-systems/, March 2013.

[4] Kamensky, J.M., *Managing the Complicated vs. the Complex*, IBM Center for the Business of Government: Washington, DC, Fall/Winter 2011.

[5] Sargut, G. & McGrath, R., Learning to live with complexity, *Harvard Business Review*, **89(9)**, pp. 68–76, 2011.

[6] Snyder, S., The simple, the complicated, and the complex: educational reform through the lens of complexity theory, *OECD Education Working Papers No. 96*, December 2013.

[7] Strauss, V. & Cuban, L., The difference between "complex" and "complicated" – and why it matters in school reform, The Washington Post, August 8, 2014.

[8] Waldrop, M.M., *Complexity: the Emerging Science At the Edge of Order and Chaos*, Touchstone, Simon & Schuster: New York, NY, 1992.

[9] Brody, P., Today's Complex Global Supply Chains are Poised to be Dismantled, *Gigaom*, July 2, 2013.

[10] Deshpande, B.R., Top 5 reasons for supply chain complexity – measuring and monitoring complexity to generate early warnings, *Ontonix*, July 2010.

[11] Shared Assessments Program, Agreed Upon Procedures (AUP) and Standard Information Gathering Questionnaire (SIG), *The Santa Fe Group*, available at http://santa-fe-group.com/capabilities/shared-assessments, 2014

[12] BITS IT Service Provider Working Group, BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, *BITS/Financial Services Roundtable*, available at http://www.bits.org/publications/vendormanagement/TechRiskFramework0210.pdf, October 2001.

[13] Shanker, D., 11 Food companies that won't tell you where their meat comes from, *BuzzFeed Life*, April 10, 2014.

[14] Axelrod, C.W., Malware, 'weakware', and the security of software supply chains, *CrossTalk Journal*, March/April, 2014.

[15] Pelgrin, W., Routh, J. & Williams, J., SANS Application Security Procurement Language, *SANS Software Security*, available at http://software-security.sans.org/appseccontract, January 2009.

[16] Axelrod, C.W., *Outsourcing Information Security*, Artech House: Norwood, MA, 2004.

[17] Axelrod, C.W., Risks of unrecognized commonalities in the information technology supply chain, *IEEE International HST Conference*, Waltham, MA, 2010.

[18] Axelrod, C.W. & Schmidt, R., A successful transaction level simulation model of the US securities marketplace, *IEEE International HST Conference*, Waltham, MA, 2012.

[19] Axelrod, C.W., Using transaction-level simulation to prepare for and recover from supply-chain disasters, *IEEE International HST Conference*, Waltham, MA, 2013.