Proceedings of the 11th International Conference on Manufacturing Research (ICMR2013), Cranfield University, UK, 19th – 20th September 2013, pp 519-524

MEASURING INFORMATION SECURITY BREACH IMPACT AND UNCERTAINTIES UNDER VARIOUS INFORMATION SHARING SCENARIOS

Olatunde A. Durowoju
Norwich Business School
University of East Anglia
Norwich Research Park
Norwich NR4 7TJ
o.durowoju@uea.ac.uk

Hing Kai Chan
Norwich Business School
University of East Anglia
Norwich Research Park
Norwich NR4 7TJ
h.chan@uea.ac.uk

Xiaojun Wang
School of Economics, Finance and Management
University of Bristol
Bristol, BS8 1TN, UK
xiaojun.wang@bristol.ac.uk

ABSTRACT

This study draws on information theory and aims to provide simulated evidence using real historical and statistical data to demonstrate how various levels of integration moderate the impact and uncertainties of information security breach on supply chain performance. We find that the supply chain behaves differently under various levels of integration when a security breach occurs. The entropy analysis revealed that the wholesaler experience the most uncertainty under system failure and data corruption. This sort of impact-uncertainty information will aid in designing and managing a resilient supply chain poised for minimal breach impact.

Keywords: Supply chain integration, Supply chain disruption, Entropy, Simulation

1 INTRODUCTION

The prevalence of this information sharing paradigm is so rampant that many organisations now cannot do without it. Any compromise to the flow of this vital information would have drastic effect on business performance. Therefore businesses and even supply chains have realised the need to protect this information, even so a significant number have not done enough to protect the Information Systems (IS) that carries this information (Potter and Beard, 2010). With the growing level of sophistication with which miscreants attack various IS, one cannot ignore the issue of IS security. In order to plan for a formidable security strategy, the impact of IS security on supply chain operations must be well understood. Knowing the impact of security breach on an organization and how this affects other members co-owning or depending on the IS would appear to be the requisite foundation to any sustainable information security policy. An information systems security breach for the most part introduces uncertainties or chaos into supply chain operations. Therefore while it is important to understand the cost impact of these breaches, it is more so imperative to establish which aspects of operation or areas in the supply chain are most vulnerable to attack. This will particularly help the supply chain prioritize 'what?' and 'where?' along the supply chain require intensified protection and what appropriate mitigation solution should be adopted. This way, the supply chain can effectively and efficiently plan its operations, optimally prepared for any eventualities. It seems intuitive that impact of security breach and the uncertainties introduced by such breaches on supply chain members would vary depending on the extent of IS dependence. However this has not been

evidenced in literature. The extent of IS dependence is conceptualised as the level of information sharing (also called information integration) in the supply chain.

This study applies discrete event simulation (DES) to investigate the impact information security breach has on supply chain performance under various information sharing scenarios. We then use the concept of entropy theory to analyse the degree of uncertainty a breach introduces to the supply chain and its members and how this affects supply chain performance. The performances being assessed are supply chain cost which includes the inventory holding cost, backlog cost and ordering cost, and do not include cost associated with damage to company's image or regulatory fines. This paper is organized as follows. Section 2 presents a brief review of relevant literature. In Section 3, the simulation experiment models are described. Section 4 summarizes the result and discussion and Section 5 concludes the study.

2 LITERATURE REVIEW

2.1 The role of information sharing

As some have suggested that the world is currently in the information age and consequently business should be conducted with this is mind. A business would thrive if it can position itself to leverage as much relevant information as possible. Communication between businesses has greatly improved over the years with the use of Information Systems (IS) such as Inter-organizational Information Systems (IOIS) and huge efforts have been invested into communication with customers as well. Fuelling this agenda is the plethora of investigations into the benefits of communication and information sharing that can be found in literature (Chan and Chan, 2009; Li et al., 2006; Zhou and Benton Jr, 2007).

Li et al. (2006) surmised that the advantage of using IOIS does not only come from efficient transaction processing and improved monitoring and information processing capacity as previous studies indicate, but also from sharing and improved access to key business information. Such key business information have been reported to be demand, inventory, supply lead time and capacity information (Kulp et al., 2004; Yu et al., 2010) and a few others. Huang et al. (2003) revealed in quantitative terms that sharing demand, inventory, and lead time information hold varied benefits depending on the level of information sharing. At the same time, several studies in literature have also shown that the derived benefits only come under the right conditions of: right information being shared at the right time in the right format by the right entities within the right environment (Chan and Chan, 2009). Since security breach in effect would compromise the right conditions of information sharing it therefore appears intuitive that the level of information sharing would affect how an incidence of security breach impact the supply chain and its members. An indication of this has been given by Durowoju et al. (2012b) but this has not been validated. This study aims to validate this and show very clearly in quantitative terms how this happens.

There have been many studies looking at IS risks to an organization and a very few have studied IS risk to the supply chain. However there is yet to be an academic study on the impact of IS disruptions on the supply chain under various conditions. The supply chain condition is defined here as the state of the chain in terms of the level of information sharing (information integration) present, the specific ordering option being used and the structure of the supply chain. It is not evident from literature how this condition mitigates or worsens these risks.

2.2 Entropy assessment of IS risk

While previous studies have estimated information security risks as a function of threat occurrence and the associated financial loss (Rees et al., 2011), only a few have employed the Entropy theory. Although the concept of using entropy as an approach to determine uncertainty has been used in literature by (Frizelle, 2002; Frizelle and Woodcock, 1995; Martínez-Olvera, 2008; Sivadasan et al., 2002), the closest previous studies have come to applying entropy as an assessment tool in security studies has been in data privacy studies such as disclosure risk assessment (Airoldi et al., 2011), measuring anonymity (Bezzi, 2007; Deng et al., 2007). The argument is that since complexity of a system (characterized by the uncertainty of a system) can be measured using entropy approach (Frizelle and Woodcock, 1995; Martínez-Olvera, 2008), and, the little is known about a random variable the more the entropy of that variable, hence the level of entropy of a security breach can be

determined once the probability of occurrence is known (Airoldi et al., 2011). The approach is to evaluate security threats using threat occurrence to work out the level of entropy each threat introduces into the system. This will help identify those threats that are hot spots to guide management decision in selecting appropriate countermeasures and mitigation solutions. While this study is not an optimality study, it provides a useful methodology to security risk assessment from a process based view where financial loss information is not known a priori. Frizelle and Efstathiou (2002) explained that high entropy can impede flow by introducing obstacles that makes supply chain operations less predictable. By inference, security breaches introduce obstacles to the flow of operation and the predictability of these breaches can help evaluate the level of chaos they introduce into the system. Airoldi et al. (2011) demonstrated that using entropy approach in estimating risk is very effective. The mathematical definition of entropy as prescribed by Shannon (1948) is a quantitative measure of uncertainty (Martínez-Olvera, 2008; Sivadasan et al., 2002):

$$H(S) = -\sum_{i=1}^{n} Pi \ \log_2 Pi \tag{1}$$

$H(S)$ is the entropy level of the system, defined here as the expected amount of information needed to describe the state of the system S , and P_i is the probability of breach i (i=1,....,n) occurring, where $P_i \geq 0$

Sivadasan et al. (2002) proposed two models for determining operational complexity under two conditions. First is complexity associated with knowing whether the system is "in control" or "not in control" denoted by the "in or not in control operational complexity index," OCI (S^{INC}) as shown in equation (2), where P is the probability of being in control. OCI (S^{INC}) is a measure of the amount of information needed to describe the "in-control" or "not in control" state of the system. The closer the probability of incidence is to 0.5, the closer the OCI (S^{INC}) value is to one.

$$OCI\ (S^{INC}) = \ -P \log_2 P - (1-P)\log_2(1-P) \tag{2}$$

Second is the complexity associated with out-of-control states, given that the system is not in control i.e. a breach has occurred. This is denoted by the "not in control operational complexity index," OCI (S^{NC}) shown in equation (3), where $P_{i/j}$ is the conditional probability computed over the "not in control" state with states i (i=1,..., n) at nodes j (j=1,..., M). This index is a measure of the amount of information needed to monitor the extent to which the system is not in control.

$$OCI\ (S^{NC}) = \ -(1-P) \sum_{j=1}^{M} \sum_{i=1}^{n} P_{i/j} \ \log_2 P_{i/j} \tag{3}$$

According to Sivadasan et al. (2002), the sum of equation (2) and (3) is the total operational complexity denoted by the operational complexity index, OCI (Stotal). It follows that the higher the operational complexity index, the higher the entropy introduced by the breach into the system and hence the more the associated information needed to manage the system and vice versa.

3 THE SIMULATION MODEL

To illustrate the impact of a security breach, we use the latest information on system failure and data corruption (SFDC) and attack on website or internet gateway (AOW) extracted from the 2012 Information Security Breach Survey (Potter and Beard, 2010). The survey was an online self-select survey with 447 respondent organizations. The respondents were security professionals. We were able to extract information on the average service disruption period caused by the breaches as well as the frequency of occurrence. This information was incorporated into our simulation model as a deterministic model. SFDC was characterised as a breach with average disruption period of five days with an average of three occurrences per year. According to the survey, the average disruption period for AOW was one day with an average occurrence of fifty four times a year. We use these two breaches to illustrate our concept.

The sequence of activities for this study is similar to the one described in (Durowoju et al., 2012b). We would refer the reader to this article for a more comprehensive detail. Information integration is modeled in this study as sharing real time demand, inventory and lead time information. We considered four scenarios of integration, one between retailer and wholesaler only (RW); that

between wholesaler and manufacturer only (WM); and one between all three (RWM). The fourth mode is the basic chain with no information being shared (BC) and it is the base mode against which all other integration levels will be evaluated. However we have improved the reliability of the previous study to 98% confidence level. The entropy scores are calculated using the steps described in (Durowoju et al., 2012a). However we have used quantity instead of cost in our evaluation of uncertainty.

4 RESULT AND DISCUSSION

4.1 Impact of breach

An ANOVA test ($p<0.05$) revealed that integration mitigates the impact of both SFDC and AOW on supply chain operating cost. Figure 1 shows that SFDC had greater impact than AOW for all information sharing scenarios. The Paired-t test ($p<0.05$) revealed that there was significant difference in the impact of SFDC between all integration modes. The RWM mode experiences the highest like-for-like increase in cost (27%) while the BC mode enjoys the least increase (at 20%) when faced with SFDC breach type. This seems intuitive as the more the supply chain depends on information, the higher the disruption caused when this information becomes suddenly unavailable. However we see that this does not hold true under AOW breach type. This is because the average service disruption for AOW is one day, which is less than the lead time between the retailer and the wholesaler (2days). Consequently the impact of the disruption is minimised and the effect of higher level of integration lessened. Therefore there is no significant difference between the impact of AOW on a chain with no form of integration (BC) and that with integration between the wholesaler and the manufacturer only (WM). There is also no difference between WM and RWM under AOW breach. This shows that RW (at 2% impact) absorbs the impact of AOW significantly more than any other information sharing scenario. In the case of SFDC breach however, the impact was highest for the full integration mode (RWM).

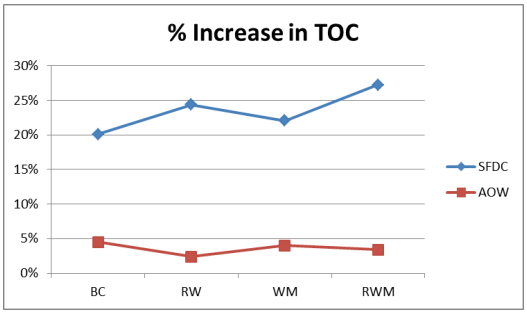

Figure 1: Impact of both security breach on supply chain operating cost

4.2 Relative effect of integration

Using the BC mode as the base mode we consider the relative effect of RW, WM and RWM. This is shown in Table 2. We find that the WM mode performs 4% better than the non-integrated chain and the other integrated chains while the RW chain performed the same as the BC mode under SFDC breach. However under AOW, the RWM mode absorbs 8% of the impact on the BC mode (which is significantly greater than WM and RW at $p<0.05$), while both WM and RW absorb 6% each of the impact on BC. We see that the mitigating effect of integration varies depending on the breach in question. It is therefore important to profile these breaches and see how they are mitigated by the supply chain condition.

Table 2: Mitigating role of integration on security breach impact

	Effect of Integration			
Breach Type	BC ($)	WM	RW	RWM
SFDD	360	4%	0%	2%
AOW	313	6%	6%	8%

4.3 Entropy assessment

The SINC is the uncertainty associated with not knowing whether there would be a negative impact or not, that is the 50/50 chance of a negative impact. The closer the probability of in-control (i.e. no negative impact observed) is to 50%, the closer SINC is to 1. Also the further the probability of in-control is from 50% either increasing or decreasing, the closer SINC is to 0. Hence the lower the SINC score the more certain you are of either experiencing a negative impact or not, the higher the score the less certain you are. The SNC on the other hand is the uncertainty associated with the number of countable states of the impact when it is negative. Higher scores occur when the impact is spread over several countable states, and lesser scores occur over few countable states. Consequently the higher the probability of experiencing a negative impact over just one single state or none at all, the closer SNC is to 0. SINC cannot exceed 1 in this case and SNC can exceed 1 depending on the spread of impact.

We see from Table 3 how the uncertainty changes for the performance of the supply chain agents depending on the level of integration when SFDC occurs. The table shows that there is no uncertainty in the way SFDC impacts the order quantity for all agents across all integration modes. However for the retailer we see that the uncertainty experienced is due to that associated with Backlog performance only and that RWM reduces this uncertainty from 0.5 in BC to 0.15. The implication is that full integration helps reduce the chaos introduced by SFDC on retailer backlog performance, while WM increases the uncertainty from 0.5 to 0.68. A further inspection indicates that this uncertainty is only due to SINC uncertainty. The incentive is for the retailer to be fully integrated with the wholesaler and the manufacturer.

For the wholesaler, uncertainty experienced in On-hand inventory performance is only due to SNC and that experience in backlog performance is due to SINC. However, we see that the RW partial integration and RWM full integration reduces the uncertainty associated with on hand inventory performance from 0.43 to zero. However WM only makes this uncertainty worse. The same trend is observed regarding the backlog performance, however the WM mode only made it marginally better instead of worse. This implies that RW and RWM would reduce the uncertainties introduced by the incidence of SFDC for the wholesaler. Therefore the incentive here might be to always integrate with the retailer and not the manufacturer only.

The influence of integration was rather different for the manufacturer. Under the on-hand inventory performance, the uncertainty brought about by SFDC was increased in the RWM scenario while decreased to zero in the RW and RWM scenarios. A similar trend is observed under the backlog performance. RWM worsens the uncertainty and WM reduces the uncertainty. Therefore the incentive for the manufacturer is to integrate with the wholesaler only.

Overall we see that the wholesaler experience the highest level of uncertainty under the BC mode (1.43) and the WM mode (1.55). The retailer experienced the least uncertainty especially under the RWM mode (0.15) the manufacturer consistently experienced more uncertainty than the retailer over all forms of integration.

Table 3: Entropy assessment of SFDC

	RETAILER				WHOLESALER				MANUFACTURER			
	Order quantity				Order quantity				Order quantity			
	BC	RW	WM	RWM	BC	RW	WM	RWM	BC	RW	WM	RWM
SINC	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SNC	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TE	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	On-Hand Inventory				On-Hand Inventory				On-Hand Inventory			
	BC	RW	WM	RWM	BC	RW	WM	RWM	BC	RW	WM	RWM
SINC	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.15	0.00	0.00	0.00
SNC	0.00	0.00	0.00	0.00	0.43	0.00	0.57	0.00	0.00	0.00	0.00	0.26
TE	0.00	0.00	0.00	0.00	0.43	0.00	0.57	0.00	0.15	0.00	0.00	0.26
	Backlog Quantity				Backlog Quantity				Backlog Quantity			
	BC	RW	WM	RWM	BC	RW	WM	RWM	BC	RW	WM	RWM
SINC	0.50	0.57	0.68	0.15	1.00	0.00	0.98	0.00	0.80	0.97	0.72	1.00
SNC	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TE	0.50	0.57	0.68	0.15	1.00	0.00	0.98	0.00	0.80	0.97	0.72	1.00
Total	**0.50**	**0.57**	**0.68**	**0.15**	**1.43**	**0.00**	**1.55**	**0.00**	**0.95**	**0.97**	**0.72**	**1.26**

4 CONCLUSION

We have only tried to show that integration mitigates the impact of security breach and demonstrate how these breaches introduce uncertainties in the performance of supply chain agents. We have shown that the impact of a breach varies depending on the type of breach and the level of integration. While it is important to understand cost impact, the uncertainties associated with this impact is also important to keep in mind. Depending on the state of the supply chain this impact can vary depending on the severity of the disruption caused by the breach and entropy theory has been applied to understand where the vulnerabilities lie. Future work would be to complete the entropy assessment of the other breach types and also investigate the role of ordering policy in mitigating the impact and uncertainty of these breaches.

REFERENCES

Airoldi, E.M., Bai, X., Malin, B.A., 2011. An entropy approach to disclosure risk assessment: Lessons from real applications and simulated domains. Decision Support Systems 51, 10-20.

Bezzi, M., 2007. An entropy based method for measuring anonymity, Third International Conference on Security and Privacy in Communications Networks and the Workshops IEEE, pp. 28-32.

Chan, H.K., Chan, F.T.S., 2009. Effect of information sharing in supply chains with flexibility. International Journal of Production Research 47, 213-232.

Deng, Y., Pang, J., Wu, P., 2007. Measuring Anonymity with Relative Entropy, in: Dimitrakos, T., Martinelli, F., Ryan, P., Schneider, S. (Eds.), Formal Aspects in Security and Trust. Springer Berlin / Heidelberg, pp. 65-79.

Durowoju, O.A., Chan, H.K., Wang, X., 2012a. Entropy assessment of supply chain disruption. Journal of Manufacturing Technology Management 23, 998-1014.

Durowoju, O.A., Chan, H.K., Wang, X., 2012b. The Role of Integration in Information Security Breach Incidents, In: Seventeenth International Working Seminar on Production Economics 2012, 20-24 February, , Innsbruck, Austria.

Frizelle, G., Efstathiou, J., 2002. Seminar Notes on 'Measuring Complex Systems'. London School of Economics.

Frizelle, G., Woodcock, E., 1995. Measuring complexity as an aid to developing operational strategy. International Journal of Operations & Production Management 15, 26-39Internat.

Huang, G.Q., Lau, S.K., Mak, K.L., 2003. Impacts of Sharing Production Information on Supply Chain Dynamics: A Review of the Literature. International Journal of Production Research 41, 1483-1517.

Kulp, S.C., Lee, H.L., Ofek, E., 2004. Manufacturer Benefits from Information Integration with Retail Customers. Management Science 50, 431-444.

Li, J., Sikora, R., Shaw, M.J., Woo Tan, G., 2006. A strategic analysis of inter organizational information sharing. Decision Support Systems 42, 251-266.

Martínez-Olvera, C., 2008. Entropy as an assessment tool of supply chain information sharing. European Journal of Operational Research 185, 405-417.

Potter, C., Beard, A., (2010). Information Security Breach Survey 2010, Information Security Breach Survey

Rees, L.P., Deane, J.K., Rakes, T.R., Baker, W.H., 2011. Decision support for Cybersecurity risk planning. Decision Support Systems In Press, Corrected Proof.

Shannon, C.E., 1948. A Mathematical Theory of Communication. The Bell System Technical Journal 27, 379-423, 623-656.

Sivadasan, S., Efstathiou, J., Frizelle, G., Shirazi, R., Calinescu, A., 2002. An information-theoretic methodology for measuring the operational complexity of supplier-customer systems. International Journal of Operations & Production Management 22, 80-102.

Yu, M.-M., Ting, S.-C., Chen, M.-C., 2010. Evaluating the cross-efficiency of information sharing in supply chains. Expert Systems with Applications 37, 2891-2897.

Zhou, H., Benton Jr, W.C., 2007. Supply chain practice and information sharing. Journal of Operations Management 25, 1348-1365.