Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 23 Issue 2 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Board Recipe for Minimizing Supply-Chain Cyber Loss

By Jason K. Deane & Wade H. Baker

Introduction- After attending corporate board meetings for approximately 85 different Fortune 500 organizations and listening to CEOs and CISOs discuss cyber risk in supply chains; and after then meeting with many of them personally, we came away with three primary takeaways. First, the main cybersecurity interest of most upper-level managers is primarily in avoiding major negative consequences (i.e., Black Swans) to their firms. Second, over 90% of corporate board members we have met with are either neutral or not confident with their security program's effectiveness. But finally, and of major concern to us, was the observation that CISOs primarily tell their boards "anecdotes" or "stories," and they do not present boards with any substantive and specific direction to avoid supply-chain cyber loss.

GJCST-E Classification: *FOR Code: 150314*

Strictly as per the compliance and regulations of:

A Board Recipe for Minimizing Supply-Chain Cyber Loss

Jason K. Deane [α] & Wade H. Baker [σ]

I. Introduction

After attending corporate board meetings for approximately 85 different Fortune 500 organizations and listening to CEOs and CISOs discuss cyber risk in supply chains; and after then meeting with many of them personally, we came away with three primary takeaways. First, the main cybersecurity interest of most upper-level managers is primarily in avoiding major negative consequences (i.e., Black Swans) to their firms. Second, over 90% of corporate board members we have met with are either neutral or not confident with their security program's effectiveness. But finally, and of major concern to us, was the observation that CISOs primarily tell their boards "anecdotes" or "stories," and they do not present boards with any substantive and specific direction to avoid supply-chain cyber loss. We believe this is unfortunate because, based on a different set of experiences we have had, namely performing several thousand forensic studies, including about one thousand for the U.S. Secret Service-most with about 100 page or more reports, we believe corporate boards can take specific reasoned actions and thereby reduce significantly their organization's exposure to, and subsequent losses from, supply-chain cyber-attacks.

To state the situation in different terms, we have found that, yes, *being in a supply chain increases your risk*. In particular, our data show that under average circumstances, by joining a supply chain, a firm increases its risk by 70%. But, *yes, it is also possible to effectively mitigate cyber risk, and if a firm doesn't, it may really pay for that non-action*. Most importantly, we have learned that *how a firm manages its risk given its membership in a supply chain does make a difference*. And we have developed a recipe for managing this supply chain cyber risk. We believe our results completely agree with the framework established by Parenty and Domret [HBR, 2019], but we in fact extend their findings to a supply-chain context. We believe corporate boards can, and need, to be involved in mitigating cyber risk and that the actions to be taken go significantly beyond the recounting of anecdotes and "stories," as we will shortly explain.

Author α: Department of Business Information Technology Virginia Tech, Blacksburg, VA 24061 USA. e-mail: jdeane1@vt.edu
Author σ: Department of Business Information Technology Virginia Tech, Blacksburg, VA 24061 USA. e-mail: wbaker@vt.edu

Very briefly, how did we arrive at this recipe? In order to understand and extrapolate from the two thousand or so forensic cyber cases we investigated, we noticed very early on that we needed to come up with a new way of recording the cyber causes and effects of supply chain risk and consequences we were seeing. Thus, we developed the *A4 Threat Model*, which provides a robust schema for describing security incidents in a structured and repeatable manner. Specifically, the A4 model records data in three major sections-Victim, Event (represented as the "4A's"-*Actor*, *Action*, *Asset*, *Attribute*), and Impact-along with some miscellaneous context about the incident itself. Thus, the A4 model essentially categorizes cyber possibilities into 378 (3 actors, 7 actions, 6 assets, and 3 attributes) distinct threat events.

The A4 model is now an industry standard; it aims to provide a database for an information security Decision Support System. With this threat model, we can constructively and cooperatively learn from our experiences to better measure and manage risk, which is especially important in tightly integrated and highly collaborative supply networks. Boards do not need to get involved in the intimate details, such as which of the 378 specific possible scenarios they need to worry about. Rather, *our* studying 2,000 forensic episodes and categorizing each into the 378 possible types, has led us to garner insight, which we are now able to both generalize and yet detail how a corporate board should get involved to minimize organizational risk.

II. The Board Recipe

Here is the basic recipe for a board to best manage its organization's supply-chain risk.

a) *Establish your Context*

Deane et al. [2022] and Parenty and Domret in a recent *Harvard Business Review* [2019] article have argued that corporate management is *not* involved, but *should get involved*, in managing corporate cyber risk in general. Then these authors provided a very insightful approach whereby they specified what they call a four-step *cyber threat narrative* explaining how the board should get involved. First, they said, the board needs to determine the organization's critical business activities and risks. This would involve interviewing company leaders, examining statements of company risk tolerance, looking at company potential sources of

major revenue, etc. Then the board must ascertain essential systems that support these critical activities; this involves getting IT to catalogue computer systems and the functionality they supply for each critical activity or risk. Thirdly, they should determine the types of cyber attacks that might harm these support systems; this involves studying and coming to understand what an adversary needs in order to pull off an attack. And finally, the board should have generated for them a list of firms or individuals most likely to be possible cyber adversaries. Parenty and Domret note that company leaders and operations staffers involved in critical business activities are best at identifying potential adversaries.

Thus, we specify that the first step in a Board recipe to minimize cyber risk in a supply chain is just Parenty and Domret's first step, namely, *as certain the threats to your organization's key activities*.

Our second step regarding cyber risk in a supply chain is for the board to have determined for it *who is in the organization's first tier of supply-chain partners*. If you are in a supply chain, you are exposed to three additional types of threats beyond the *direct threats* you are subjected to when not belonging to a chain. We have observed that the biggest by far of the three new types of threats you face beyond the direct attack when you join a chain is the *partner vector* threat. The board should be aware, however, that even more significant than the new partner vector threat is the (old) direct threat. This direct threat still will constitute most of your risk, so you must continue to follow the Parenty-Domret advice as a first step. But a vector threat occurs because you are electronically connected to your supply-chain partners, and so you may experience the results of an attack because you are just connected to some other firm with a whole different set of critical business activities and risks, cybersecurity types, and cyber adversaries.

Depending on how big a supply chain you belong to, you may have first-tier partners, who are in turn connected to *their* first-tier (and your second-tier) partners, who in turn are connected to *their* first-tier (and your third-tier) partner. We have observed over the years that focusing on just your first-tier of partners will mitigate much of your risk.

Therefore, the board must expand its focus beyond just the *organization's* four aspects of its own cyber narrative (its set of key activities, associated essential support systems, associated collection of types of possible cyber-attacks, and finally its cyber adversaries). The board must also attempt to gain insight either directly from its supply-chain partners if they are willing and able to do so; or the board must have generated for it an in-house estimate of each first-tier partner's cyber narrative. Then, with these inputs, the board should focus to the extent possible on the set of four factors for each of its first-tier suppliers as for itself.

In short, an organization should first establish an extended context consisting of itself and its first-tier partners.

b) Reduce Vector Attacks

If an organization has a breach of any type or source, there is a probability that the breach will "propagate" to all partners in the network connected to the original victim. Thus, by connecting in a supply chain, a firm may incur the "side-effects" of any of its partners being breached; this type of breach is called a *partner vector breach*, or a *vector breach* for short.

There are quite a few factors that influence an organization's monetary loss from a vector attack, including its *IT* integration level; information sharing: scope/confidentiality; information sharing: degree; *its* security posture to each partner; and its partners' security postures facing them. However, we have found from our forensic analyses that, *of all these factors*, in general the most effective way to mitigate vector loss is to establish a *strong security posture* that blocks possible interference from each partner due to the electronic conduit between you two. In the many cases we examined, we found that cyber loss can vary from 1.8 times the normal value down to 0.5 times the normal risk due to this one factor alone.

A well-known example illustrating a vector attack is the case of Target and an HVAC supplier that Target also made a connected partner. In short, Target allowed an HVAC supplier in 2013 to connect electronically to it, and as a result, Target was hacked after Thanks giving and before Christmas by a third party that got into Target via the HVAC connection. The personal information (including credit card numbers) of approximately 40 million customers led to losses to Target estimated as high as $300M [Krebs, 2014] [Lynch, 2017].

In summary, *a corporate board should make sure, particularly for its supply-chain partners for whom it has inadequate information on their cyber narratives, that its security posture facing each of those partners is strong.* This is an organization's best first step in reducing partner vector breaches.

There is one more issue regarding reducing vector attacks that should provide a general caveat to a board: *The industry to which a partner belongs will affect the type of attack you experience*.

We have plotted in Figure 1 the types of cyber-attacks *experienced* over the years in various industries. Each dot in Figure 1 represents an industry subsector identified by a three-digit North American Industry Classification System (NAICS) code. Subsectors within the same higher-level sector are grouped by color (i.e., several retail (44x) subsectors in the upper right are all

grey). The size of the dot corresponds to the number of breaches recorded for that subsector (larger = more). The distance between the dots shows how breaches in one subsector compare to that of another. If dots are close together, it means breaches in those subsectors share similar A4 Threat Model characteristics (in terms of actors, actions, assets, and attributes). If far away, it means the opposite. In other words, subsectors with similar breach profiles appear closer together.

Now, for example, suppose you are an organization in the industry *Manufacturing* and that you have insured that you are well protected against the type of threats experienced by firms in the center of Figure 1. Then if you join a supply chain with a firm that provides *Transportation and Warehousing (Distribution)*, you have now become exposed to a whole new potential category of threats and attacks because, as the figure shows, Transportation and Warehousing is in the upper left corner of the cluster plot of threat types.

As an organization, you most likely will *not* be able or even want to exclude another organization because of the industry to which it belongs; in fact, its industry is probably why you want that organization in your chain. So the caveat we offer here is that, as a board, you should be aware that if you have supply-chain members in portions of Figure 1 distant from your industry, you will want to pay extra attention to those members and determine the types of attacks more common to them than to you.

c) *Simplify Electronically the type of Chain to which you belong*

The next step in the recipe to cyber-risk success is that boards should insist that the information sharing structures of organizations in the chain, i.e., the electronic connections between its own organization and all partners, should be simplified as much as possible.

In our experiences, we have observed cyber-attacks on supply chain members connected electronically in many different configurations. The literature lists and names some common connectivity schemes, and we have shown three of the most common in Figure 2. From left to right in that figure are examples of "linear (sequential)," "hub-and-spoke," and "reciprocal" connectivity strategies. [See, e.g., Liu and Kumar (2003)]. Note for example, that in the reciprocal connectivity chain, essentially everyone is connected to everyone else; this results in way more connections than in, say, a simple linear (sequential) arrangement. Of course, it must be recognized that oftentimes the type of connectivity must be specified due to business purposes other than cyber considerations. But what we have observed over the years from our forensics is that the way firms connect, taken together with their security postures, greatly affects cyber loss. For example, we have seen five firms connected reciprocally with poor security posture experiencing over one billion dollars more loss over five years than five similar firms connected with strong security.

In short, *a corporate board should thus, to the extent possible, reduce the number of inter-firm electronic connections.* If it is absolutely necessary to connect everyone to almost everyone else, the board must insist to IT that *its security posture facing every such partner is as strong as possible.*

d) *Force your Partners to be Responsible*

There is a somewhat surprising piece of evidence that makes this final measure of the board recipe not only an important step, but in fact, an essential one. The action? to the extent you are able, *force your partners to improve their security posture toward you in particular, and also toward the world in general*. Our experience has clearly demonstrated that, when I am in a supply chain, my risk as a firm is *not* the same as all my partners' risk. In fact, we have seen over and over that *risk in a chain is not commensurate with culpability*. Our findings clearly indicate that the firm that causes most of the risk does *not* necessarily incur the most risk. That is, in some cases, some other firms incur more risk than even the "weakest link."

It thus is worthwhile for a firm to help-or even demand that (if possible)-its partners obtain a strong security posture. This recommendation is not unlike what occurred in the early dot-com era when large firms like Wal-Mart required and/or incentivized suppliers to modernize IT systems to reduce overall risk.

III. Conclusions

As Parenty and Domret [2019] and Deane et al. [2022] have argued, historically, corporate management has *not* been involved, but now can and *should get involved*, in managing corporate cyber risk in general. This present work shows that extending the Parenty-Domret work to supply chains is also an activity that corporate boards can and should be involved in.

In particular, this paper suggests the manner in which boards should take leadership in order to reduce cyber attacks on its organization due to its membership in a supply chain:

First, Eextend your Parenty-and-Domret Context

Now you must also include your first-tier partners in your "context."

Next, Reduce your Vector Threats

The way to do this is to establish a *strong security posture* that blocks possible interference from each partner due to the electronic conduit between you two. Also watch out for industries distant from yours in an A4 sense (see Figure 1).

Third, Simplify Electronically your Information Sharing

Reduce the connectivity (see Figure 2) among chain members as much as practical. When denser connectivity is necessary for other than cyber reasons, be especially careful, once again, to mandate that the appropriate IT groups increase your security facing each firm.

Finally, "force" Partners to be Responsible

Since cyber loss is not proportional to cyber culpability, the board should help and/or force partners to improve their security posture toward both you and the world in general.

References Références Referencias

1. Deane, J., Baker, W. and Rees, L. (2022). "Cybersecurity in Supply Chains: Quantifying Risk,"
2. *Journal of Computer Information Systems*, available online: https://www.tandfonline.com/doi/full/10.1080/08874417.2022.2081882, accessed 14 December 2022.
3. Krebs, Brian. (2014). "Target Hackers Broke in Via HVAC Company, "https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/, accessed 07December 2019.
4. Liu, E. R. and Kumar, A., 2003, "Leveraging Information Sharing to Increase Supply Chain Configurability." In *Twenty-Fourth International Conference on Information Systems*, 523–537.
5. Lynch, Vincent (2017), "Cost of 2013 Target Breach Nears $300 Million, "https://www.thesslstore.com/blog/2013-target-data-breach-settled/, accessed 07 December 2019.
6. Parenty, Thomas J., and Domret, Jack J., 2019, "Sizing up Your Cyber Risks, "*Harvard Business Review*, November-December.

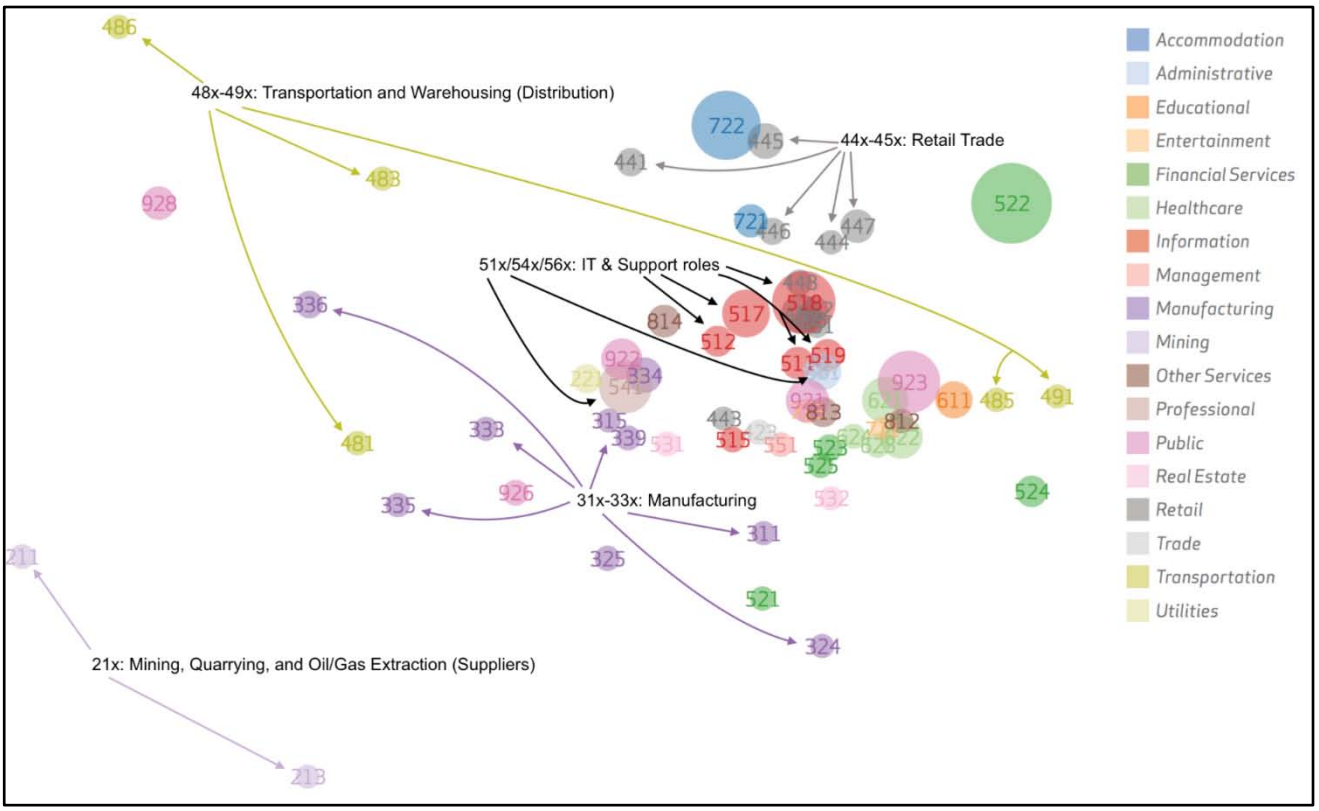

Figure 1: Cluster Analysis Showing Risk Profiles by Industry

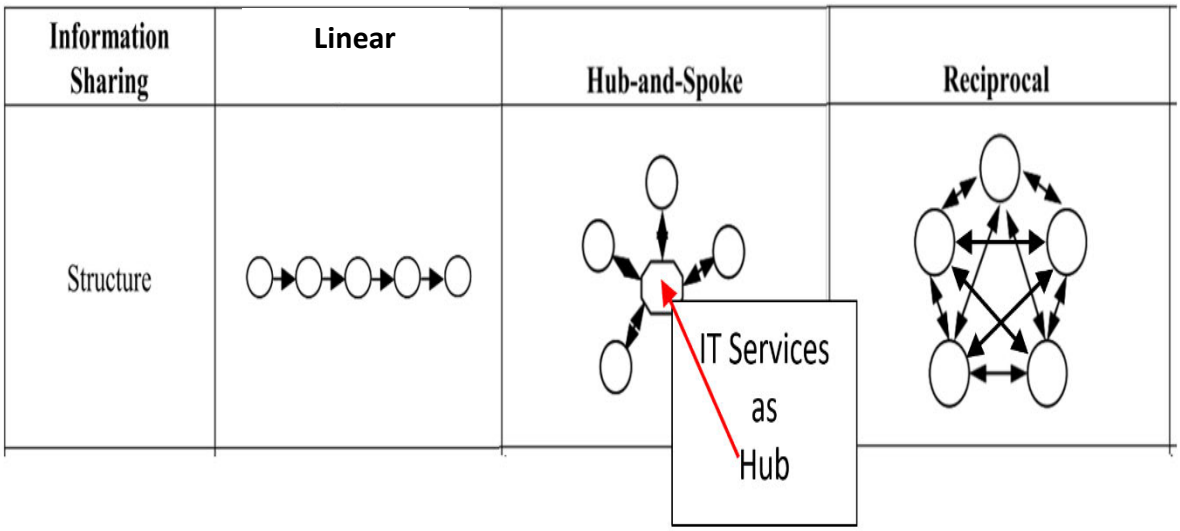

Figure 2: Three Basic Information Sharing Structures Commonly Recognized in the Supply Chain Management Literature. Taken from Liu and Kumar (2003)