Check for updates

# The economics of ransomware attacks on integrated supply chain networks

ANNA CARTWRIGHT**, Oxford Brookes University, UK
EDWARD CARTWRIGHT, De Montfort University, UK

We explore the economics of ransomware on production supply chains. Integrated supply chains result in a mutual-dependence between firms that can be exploited by cyber-criminals. For instance, we show that by targeting one firm in the network the criminals can potentially hold multiple firms to ransom. Overlapping security systems may also allow the criminals to strike at weak points in the network. For instance, it may be optimal for the attacker to target a supplier in order to ransom a large producer at the heart of the production network. We introduce a game theoretic model of an attack on a supply chain and solve for two types of Nash equilibria. We then study a hub and spoke example before providing simulation results for a general case. We find that the total ransom the criminals can demand is increasing in the average path length of the network. Thus, the ransom is lowest for a hub and spoke network and highest for a line network. Mitigation strategies are discussed.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; **Economics of security and privacy**.

Additional Key Words and Phrases: Ransomware, Network security, Supply chain, Economics, Game theory.

## 1 INTRODUCTION

Crypto-ransomware is a fast evolving cyber security threat in which criminals encrypt a victim's files and then demand a ransom for the key to decrypt the files [3, 11, 42]. Ransomware is an active threat to businesses and other organisations [33, 40, 43, 51]. Indeed, modern strands of ransomware, such as Maze, Hive and LockBit, have actively targeted businesses with devastating effect in terms of both disruption to services and ransoms raised. Ransomware (in a more sophisticated form) has only been in the wild for less than 10 years and the speed with which the threat has evolved is outpacing the development of traditional security controls and behaviors. Moreover, the criminals are clearly evolving their strategy, not only in terms of the technology behind the ransomware but also their economic strategy and business model of extortion [22, 32]. In this paper we highlight and explore how the criminals' economic strategy may develop yet further in the exploitation of supply chains.

In modern economies, complex supply chains are integral to the production of almost all goods and services, ranging from cars to food to health care. Increasingly, supply chains are global, linking production in less developed countries with consumption in developed countries [34]. Supply chains are, by their nature, inter-dependent systems in which disruption to one firm can have substantial repercussions across the whole chain [30, 47]. A cyber-attack on one link in the chain can, thus, have an amplified impact. Most basically, disruption to supply in the network will impact overall production of all up-stream firms [5, 48]. Firms may also have overlapping information or security systems meaning that a breach can propagate from one firm to another in

*Both authors contributed equally to this research.

Authors' addresses: Anna Cartwright, p0088704@brookes.ac.uk, Oxford Brookes University, Headington Campus, Oxford, UK; Edward Cartwright, De Montfort University, Leicester, UK, edward.cartwright@dmu.ac.uk.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
© 2023 Copyright held by the owner/author(s).
2576-5337/2023/2-ART
https://doi.org/10.1145/3579647

Just Accepted

the supply chain [6, 19]. Furthermore, the recovery response to a cyber-attack often involves complex interaction across sites [21].

Two examples illustrate the diverse ransomware threat to supply chains. In early 2022, Toyota was forced to halt production at its plants in Japan after an attack on one of its key suppliers, Kojima Industries [2]. In this case Toyota suffered business disruption because of the breach at a direct supplier and, given the close connections between the firms, saw potential disruption to its own IT systems. Our second example concerns Expeditors, a major freight forwarder, who was also hit by an attack in early 2022. This led to the suspension of key operations, such as booking new shipments. The resultant disruption had a knock on effect for global supply chains and all of the firms that were relying on Expeditors for timely shipment of goods. In this case, the many firms who were reliant on Expeditors will have suffered disrupted business operations because of a breach that affected the flow of goods along a supply chain. Unfortunately, ransomware attacks on logistics and manufacturing firms are becoming increasingly common [25]. Supply chains require, therefore, a highly coordinated cyber security approach that takes into account the various spillover effects [10, 45]. To inform this response it is vital that we study in detail the economic threat that a cyber-attack poses to supply chain networks.

In this paper we will demonstrate that ransomware on supply chains can have profound implications for the economic strategy that ransomware criminals can exploit. The potential for malware, including ransomware, to spread through supply chain attacks is widely acknowledged [4, 49, 50]. Indeed, two of the most well known ransomware attacks - WannaCry and NotPetya - gained notoriety in large part because they infiltrated supply chains. WannaCry directly impacted the UK National Health Service with knock on effects for a range of downstream health services [23]. NotPetya spread through the use of tax accountancy software and disrupted a range of essential services, particularly in Ukraine, including banks and electricity production [46]. The SolarWinds attack in late 2020 is another example of malware spread through software updates [41]. Our focus in this paper, however, is not on the propagation of ransomware but on the ransoms that can be demanded. As ransomware attacks on supply chains continue to evolve and grow it is natural that economic strategies will also evolve. We will show that the inter-dependency along a supply chain means that criminals can charge higher ransoms when firms are in a supply chain. Moreover, the criminals could attack one firm in the network and hold another to ransom, or they could hold multiple firms to ransom at the same time. The REvil/Sodinokibi attack on Apple's supply chain illustrates that such tactics are more than a theoretical possibility [17]. In this case the attackers breached Quanta Computer but then targeted Apple for a $50 million ransom.

To study the effects of ransomware we shall use a game theoretic approach in which we derive the optimal ransom, or, equivalently, the maximum ransom that affected firms would be willing to pay [9, 16, 29, 32]. The optimal ransom is shown to depend on the characteristics of the supply network and also the ability or willingness of firms to coordinate a response to the criminals. We provide general results detailing the Nash equilibrium ransom demands and apply this to a hub and spoke network. Our work builds on existing game theoretic studies of cyber security on supply chains [12]. It also offers a framework with which to model and improve the cyber-resilience of supply chains. A large literature addresses the general issue of supply chain resilience [26, 37, 38]. One strand of this literature looks at network structure [31]. Our model allows insight of the type of network structure that would reduce the level of any potential ransomware demand. In particular, we show that the amount of ransom the criminals can extract depends critically on the average path length between firms in the supply chain.

Our approach abstracts away from the moral and negative social consequences of firms paying ransoms. Ransom payments to criminals fuel future ransomware attacks and criminality. From a societal point of view they are clearly, therefore, undesirable. Indeed, there have been calls to ban ransomware payments [1, 14]. There are, though, complex trade-offs for a firm in assessing the benefits and costs of a ransom payment [15, 24, 52]. And the simple reality is that many firms impacted by a ransomware attack have incentives to pay and do pay [39]. A game theoretic approach allows us to model that incentive to pay. Moreover, it allows us to explore

Just Accepted

characteristics of the supply network that would lower the ransom that victims are willing to pay, and thus alleviate the ransomware threat. It also allows us to preempt future strategies the criminals may adopt. Our results, as we discuss, thus, provide a framework to explore potential mitigation measures that supply chains can use.

We proceed as follows: In Section 2 we introduce the model and notation. In Section 3 we provide our main theoretical results. In Section 4 we consider hub and spoke networks while in Section 5 we simulate more general network structures. In Section 6 we conclude.

## 2 MODEL

### 2.1 Supply network

We consider a supply chain involving a finite set of firms $N = \{1, ..., n\}$. The supply chain can be described as a network consisting of set of nodes $N$ and a weighted adjacency matrix $A \in [0, 1]^{n \times n}$ where $a_{ij}$ indicates the dependence of firm $i$ on the production of firm $j$. The precise interpretation of $a_{ij}$ will be explained shortly but, informally, if firm $j$'s production is completely disrupted by cyber attack (or other reason) then the output of firm $i$ is reduced by a factor $a_{ij}$. Thus, $a_{ij}$ is a measure of how much form $i$ relies on firm $j$ or, equivalently, how much a disruption at firm $j$ would impact firm $i$. For example, if $a_{12} = 1$ and firm 2 is unable to produce because of a cyber attack then firm 1 would also be unable to produce until the attack is resolved. If $a_{12} = 0.5$ then firm 1 would be able to produce half its normal output. This allows us to capture, for example, the impact that the attack on Kojima Industries had on Toyota, or that on Quanta Computer had on Apple.

Throughout, we assume the supply network is a directed acyclic graph. In interpretation, this means production flows from periphery firms to intermediaries to a central producer. This assumption is consistent with the supply chain to a large manufacturing business where the manufacturer sources components from suppliers. Figure 1 provides an example with 5 firms. Firms 5 and 4 supply to intermediaries 3 and 2 which, in turn, supply to firm 1. For instance, firm 1 may be a car manufacturer that relies on a chain of suppliers for wheels, seats and engine parts etc. The adjacency matrix in this case is

$$A = \begin{array}{c} \text{Supplier} \\ \\ \\ \\ \\ \\ \end{array} \begin{pmatrix} 0 & 0.1 & 0.2 & 0 & 0 \\ 0 & 0 & 0 & 0.1 & 0 \\ 0 & 0 & 0 & 0.1 & 0.2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{1}$$

For instance, $a_{13} = 0.2$ means that firm 1s output would lower by 0.2 if firm 3 was unable to operate. Generally speaking, we can think of $\overline{A} = \sum_{ij} a_{ij}$ as a measure of the inter-dependence and inter-connectedness of the supply chain.

When the supply chain is fully functioning we represent the output of firms, measured in monetary units per period of time, by column vector $V = [v_1, ..., v_n]^T$ where $v_i$ is the output of firm $i$. We model a cyber-attack on the supply chain by vector $K = [k_1, ..., k_n]$. The value $k_i \in [0, 1]$ measures the fractional reduction in output of firm $i$ as a *direct* result of the attack. Hence, the output of firm $i$ is reduced from $v_i$ by amount $k_i v_i$ to $(1 - k_i)v_i$. If, for instance, $K = [0, 0, 0, 0.5, 0]$ then the attack directly reduces the output of firm 4 by a half. Crucially, our modelling framework allows for a simultaneous attack on multiple firms. For instance, it could be that $K = [0, 0, 0.5, 0.5, 0.5]$ indicating that the attack directly reduces the output of firms 3, 4 and 5 by a half. This allows us to capture the potential for overlapping IT systems in which a breach in one firm propagates to other firms in the supply network causing wider disruption [44]. It also allows us to model an attack on, say, a logistics firm which directly impacts multiple firms across a supply network.

Just Accepted

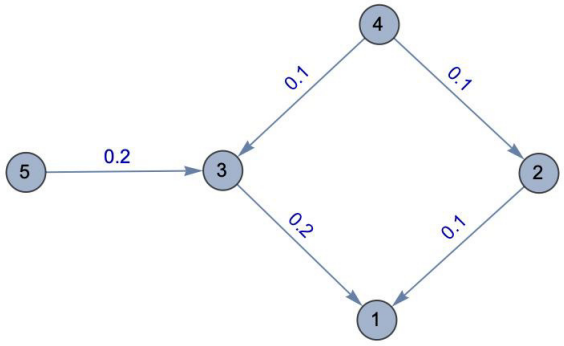



Fig. 1. Example of a supply network with five firms.

Because firms are in a supply chain the direct effects of the attack will ripple through the network. The adjacency matrix $A$ allows us to capture this ripple effect. We assume that the effects are additive across firms (subject to output being non-negative). To illustrate, suppose in the example of Figure 1, that an attack on firm 4 reduces its output by a half, $K = [0, 0, 0, 0.5, 0]$. This will reduce output of firm 2 by factor $a_{24}k_4 = 0.1 \times 0.5 = 0.05$ and also output of firm 3 by factor 0.05. This, in turn, will reduce output of firm 1 by $(a_{12}a_{24} + a_{13}a_{34})k_4 = 0.1 \times 0.05 + 0.2 \times 0.05 = 0.015$. Generally speaking, the total effect of an attack $K$ on the supply network can be calculated as column vector

$$C = \sum_{i=0}^{n} A^i K^T \tag{2}$$

where $c_i$ measures the overall factor by which the output of firm $i$ is cut during the attack. In the following we assume that $c_i \leq 1$ for all $i$.[1] The output of firm $i$ during the attack is given by $(1 - c_i)v_i$.

To illustrate, consider again the example of Figure 1. If $K = [0, 0, 0, 0.5, 0]$ then the cumulative effect is $C^T = [0.015, 0.05, 0.05, 0.5, 0]$ and so output during the attack is given by $[0.085v_1, 0.95v_2, 0.95v_3, 0.5v_4, v_5]$. The reduction in output of firm 4, thus, directly impacts the output of firms 2 and 3 which then impacts the output of firm 1. As a second illustration, suppose that $K = [0, 0, 0.5, 0.5, 0.5]$ indicating that firms 3, 4 and 5 are hit by a cyber attack. Then $C^T = [0.135, 0.05, 0.65, 0.5, 0.5]$ is the cumulative effect across the supply chain. For example, firm 3 suffers the effect of its own attack and the ripple effect from firms 4 and 5 also being attacked. Output during the attack is given by $[0.865v_1, 0.95v_2, 0.35v_3, 0.5v_4, 0.5v_5]$. We see, for example, that firm 2 is less affected than firm 1 by the attack because it is directly and indirectly less reliant on suppliers down-stream.

## 2.2 Ransomware game

We model a cyber-attack on a supply chain as a dynamic game, following the approach of Cartwright et al. (2019) [9]. The game involves $n + 1$ players - the $n$ firms in the supply network and a criminal gang. To focus the analysis we take as given an exogenous cyber-attack $K = [k_1, ..., k_n]$, meaning that the criminals have successfully breached at least one firm in the supply chain. We then focus on the optimal ransom, from the perspective of the criminals, given the breach.

Before we detail the timing of the game that we will study, we note that the criminal gang and, to a lesser extent, the firms have considerable control over the 'rules of the game'. For instance, the criminals can determine the conditions under which they will restore functionality of the supply chain. Similarly, the firms can determine

[1] If $c_i > 1$ then we simply reset $c_i = 1$.

Just Accepted

the extent to which they will communicate and bargain with each other about ransom payments during the attack. To perform the game theoretic analysis we need to tie down those 'rules'. We do so in a way that we believe captures salient aspects of likely attacks. We will expand on this point, and discuss alternatives, as we proceed.

The game we study consists of the following two stages.

Stage 1: The criminal gang chooses a ransom profile $R = [r_1, ..., r_n]$. This details the ransom amount $r_i \geq 0$ that will be asked of each firm. The criminals could ask a ransom of either only one firm or ask for ransoms from multiple firms. Let $S = \sum r_i$ denote the total ransom requested across all $n$ firms by the criminal gang.

Stage 2: Each of the $n$ firms independently and simultaneously decide whether or not to pay the ransom. This is an all or nothing decision. Let $D = [d_1, ..., d_n]$ denote choices where $d_i \in \{0, 1\}$ is the choice of firm $i$ to not pay or pay the ransom asked of them.

Payoffs are determined relative to vector $D$. The total ransom paid is given by $g = RD^T$. If all ransoms are paid, meaning $g = S$ (or, equivalently, $d_i = 1$ for all $i$ such that $r_i > 0$), then the criminal gang returns functionality to the supply chain: The payoff of the criminal gang is $g$ and the payoff of firm $i$ is $v_i - r_i$. Thus, the criminals receive the ransom and the firms receive their normal output minus the ransom paid. If at least one firm does not pay the ransom meaning $g < S$ (or $d_i = 0$ for some $i \in N$ where $r_i > 0$) then we assume the criminals do not return functionality to the supply chain: The payoff of the criminal gang is $g$ and the payoff of firm $i$ is $(1 - c_i)v_i - r_i d_i$. In this case the firms suffer lower output because of the attack. Also some firms may have paid the, non-recoverable, ransom.

The payoff function set out above is built around an assumption that the criminals restore full functionality of the network if and only if *every firm* asked to pay a ransom does so. There are a number of alternative assumptions we could have made. For instance, it could be the case that the criminals will not return access even if the ransoms are paid, or that the systems are so corrupted that access cannot be restored [8]. Or, it could be the criminals return access to those firms which do pay the ransom and not those who do not pay. Moreover, in practice, we observe ransom amounts are typically negotiated with offers and counter-offers made by victims and the criminal gang. A game theoretic approach abstracts away from such negotiations by assuming that the ransom demands $R$ are the predictable endpoints of the negotiation [20]. With this in mind, we believe our assumption, that the criminals will restore functionality if and only if the total ransom amount is paid, appears broadly consistent with the current behavior of ransomware criminals.

Another assumption underlying our model is that any firm $i$ asked to pay a positive ransom ($r_i > 0$) knows the attack profile $K$ and the ransom profile $R$. This means they know the firms affected by the attack. We, thus, assume an element of common knowledge amongst those ransomed. A firm that is attacked may have reputational motives to 'hide' an attack [27]. The nature of a supply chain means, however, that a cyber-attack is difficult to 'hide'. In particular, in our model, an attack disrupts production in a way that would be noticed down the chain. The only way that a firm could 'hide' the attack would, thus, be to claim some other cause for the disruption. Even this wiggle room may be disrupted by the criminals. In particular, the criminals can inform all firms in the supply chain of $K$ and $R$, or publicize the attack more widely. Given that this allows the criminals to potentially increase the ransom demand it is in their interests to do so. The example of Quanta Computer and Apple, discussed in the introduction, illustrates this possibility. We, thus, consider it mild to assume that $K$ and $R$ are common knowledge amongst those affected.

The final preliminary we explain about our model is the assumption that specific ransom amounts are identified for individual firms. The results to follow are in no way dependent on this assumption. In particular, we could equivalently consider a stage 1 in which the criminals make an aggregate ransom demand of $S$ and a stage 2 in which the firms independently decide how large a ransom they are willing to pay. The criminals then restore full functionality if and only if the total ransom paid is greater than or equal to the ransom demand. We have

Just Accepted

adopted an approach that takes account of firm specific demands to provide more transparency on the ransom each firm will pay in equilibrium.

## 3 THEORETICAL RESULTS

To determine the optimal strategy of the criminals, we use backward induction to solve for sub-game perfect Nash equilibria of the game. A sub-game perfect Nash equilibria consists of a strategy for the criminal gang and the firms such that, at any decision point, each of the players maximize their own payoff given the strategies of others [18]. In applying backward induction we determine the optimal strategy of the firms (in stage 2 of the game) for any feasible ransom demand, and then subsequently determine the optimal ransom demand (in stage 1 of the game). Given that payment of the ransom will restore functionality of the supply chain, firms have an incentive to pay the ransom if the ransom is sufficiently low. Thus, it is in the interests of the criminals to determine the maximum ransom that firms are willing to pay.

In stating our first result we define $\epsilon$ as the smallest unit of currency in the economy. Our first result provides an upper bound on the ransom that the criminals can receive in equilibrium.

Theorem 3.1. *Take as given cyber-attack $K = [k_1, ..., k_n]$. It is a sub-game perfect Nash equilibrium for: (a) the criminals set ransom $r_i = v_i c_i - \epsilon$ for all $i \in N$ such that $c_i > 0$, and (b) for every firm $i \in N$ to pay the ransom, $d_i = 1$.*

Proof. Consider stage 2 of the game. Fix a ransom profile $R = [r_1, .., r_n]$ and firm $i \in N$. Suppose that $d_j = 1$ for all $j \in N, j \neq i$ such that $r_j > 0$. If firm $i$ pays the ransom the attack is resolved and firm $i$ has payoff $v_i - r_i$ If firm $i$ does not pay the ransom the attack persists and firm $i$ has payoff $v_i(1 - c_i)$. It is, therefore, optimal for firm $i$ to pay the ransom if and only if $r_i < v_i c_i$.[2]

We say that ransom profile $R$ is incentive compatible if $r_i < v_i c_i$ for all $i \in N$. Extending the logic of the preceding paragraph it is consistent with sub-game perfection that every firm $i \in N$ pays the ransom if and only if the ransom profile is incentive compatible.

Consider the criminals in stage 1 of the game. If the criminals choose a non-incentive compatible ransom profile then his payoff is 0. If the criminals choose an incentive compatible ransom profile $R$ then his payoff is $S = \sum_i r_i$. It is, therefore, optimal to choose the incentive compatible ransom that maximizes $S$. This is given by $r_i = v_i c_i - \epsilon$ for all $i \in N$. □

As one would expect, Theorem 3.1 shows that the total ransom the criminals can demand is increasing in the disruption caused by the attack (as given by $k_i$ for all $i$) and the inter-connectedness of the supply chain (as given by $c_i$ for all $i$ which, in turn, depends on $\overline{A}$). For instance, the criminals can demand a higher ransom if they are able to propagate a breach across overlapping IT systems, meaning $k_i > 0$ for multiple $i$, than if they are only to breach one firm in the supply chain. Similarly, the criminals can demand a higher ransom if the firms in the supply chain are highly dependent on each other for production.

There are two important novelties to Theorem 1 that we want to emphasize: (i) The criminals may charge a ransom and the firm may pay even if the ransom exceeds the direct impact of the attack on the firm. This will be the case if $c_i > k_i$. Previous work on the economics of ransomware has only considered the direct impact of an attack and so may underestimate potential ransom demands [7, 9]. Indeed it may be that $k_i = 0$ meaning that the firm suffers no direct impact at all from an attack and yet would still pay a ransom because of the indirect disruption to production. (ii) It may be optimal for the criminals to ransom multiple firms from one attack because multiple firms are impacted.

Points (i) and (ii) can be illustrated with the example of Figure 1 and attack vector $K = [0, 0, 0, 0.5, 0]$. The optimal ransom profile in this case is $R = [0.015v_1, 0.05v_2, 0.05v_3, 0.5v_4, 0]$. Thus, an attack on firm 4 allows the

[2]We assume that if $r_i = v_i c_i$, and so firm $i$ is indifferent between paying and not paying, it will not pay.



Just Accepted

criminals to ransom firms 1, 2 and 3, as well as firm 4. The criminals are able to ransom firms 1, 2 and 3, despite them not being directly attacked, because the attack on firm 4 is disrupting their output. This type of strategy seems plausible in the field, and not just a theoretical possibility, given that criminals appear to be increasingly targeting supply chains because of the disruption such attacks can cause [4, 49, 50]. Indeed, the examples we gave in the introduction, of breaches to Quanta Computer and Kojima Industries that disrupted, respectively, Apple and Toyota, are consistent with the strategy we are outlining.

Theorem 3.1 shows that the criminals can increase their revenue by strategically attacking supply chains and setting appropriately high ransoms. The strategy of making an 'all or nothing' ransom demand also, though, carries a risk. In particular, it requires victims to coordinate in a way that stage 2 of the game is equivalent to a minimum effort or weakest link game [13, 28]. If one firm in the supply chain does not pay the ransom then the criminals will not restore functionality of the supply chain; hence, it is not in the interests of other firms to pay the ransom either. There is, therefore, the potential of 'coordination failure' in which firms do not pay the ransom because they do not expect other firms to pay the ransom. This is a 'coordination failure', from a game theoretic point of view, because the firms would collectively be better off to pay the ransom, but fail to coordinate on how to do so.

If coordination failure is likely then it is not in the interests of the criminals to ransom multiple firms. Instead they should ransom the firm in the network that will suffer most from the attack. This is encapsulated in our second result.

Theorem 3.2. *Take as given cyber-attack $K = [k_1, ..., k_n]$. Let $i \in N$ be the firm with maximal $v_i c_i$. Then it is a sub-game perfect Nash equilibrium for (a) the criminals set ransom $r_i = v_i c_i - \epsilon$ for $i$ and set $r_j = 0$ for all other $j \in N$, and (b) for firm $i$ to pay the ransom, $d_i = 1$.*

Proof. Consider stage 2. Fix a ransom profile $R = [r_1, .., r_n]$. Suppose that $r_l, r_j > 0$ for some $l, j \in N, l \neq j$. If $d_j = 0$ then access will not be returned irrespective of whether firm $l$ pays the ransom. Hence, it is optimal for firm $l$ to also set $d_l = 0$. Generalising, it is a Nash equilibrium of the resulting sub-game for players $l$ and $j$ to set $d_l = d_j = 0$. This is a coordination failure. It results in the criminals obtaining no ransom payments. Thus, there is no incentive for the criminals to ransom multiple firms.

Suppose the criminals set the ransom demand stated in part (a) of the Theorem. If firm $i$ pays the ransom their payoff is $v_i - r_i = v_i(1 - c_i) + \epsilon$. If firm $i$ does not pay the ransom their payoff is $v_i(1 - c_i)$. Thus, it is in the interests of firm $i$ to pay the ransom. Given that firm $i$ was chosen because it maximizes $v_i c_i$ it also maximizes revenue for the criminals (conditional on coordination failure if more than one firm is attacked). Hence it is optimal for the criminals to choose the ransom profile stated in part (a) of the Theorem. □

Theorem 3.2 reinforces point (i) in that we again see it can be optimal for the criminals to set a ransom demand which exceeds the direct impact for the firm. Point (ii) is now qualified by considerations of strategic risk. Ransoming multiple firms may result in a coordination failure in which none of the firms pay the ransom (even though collectively they may have been willing to do so). The criminals, thus, need to weigh up whether it is better to ransom one or multiple firms in the network. This could depend on the information the criminals have, such as whether the firms share the same cyber-insurer or ransom negotiator, and whether they believe they could engineer coordination in some way, such as through coordinated negotiation. The criminals may also want to consider other factors. For instance, some firms may have a greater ability to pay a ransom because of cashflow levels or their willingness to engage in ransom negotiations.

To illustrate the preceding discussion consider the example of Figure 1 with attack vector $K = [0, 0, 0.5, 0.5, 0.5]$. Also set $v_2 = v_3 = v_4 = v_5 = 1$ and $v_1 = 10$. If we apply Theorem 3.1, and so the criminals ransom multiple firms, the optimal ransom profile is $[1.35, 0.05, 0.65, 0.5, 0.5]$. The total ransom demanded is, therefore, 3.05. If we apply Theorem 3.2, and the criminals are unwilling to risk ransoming multiple firms, the optimal ransom profile will

Just Accepted

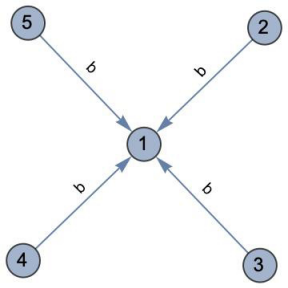



Fig. 2. Example of a hub and spoke supply network with five firms.

depend on $max_i\{c_i v_i\}$. The criminals should identify and ransom the firm with the biggest drop in output because of the attack. This need not be the firm most disrupted. Indeed, it is optimal to ransom firm 1, for 1.35, even though firm 3 faces the biggest disruption to output. This is because firm 1 has much larger output and so stands to lose more financially from the attack, even if the relative level of disruption is smaller. We see, therefore, that the criminals may want to target firms 3, 4 and 5 in order to ransom firm 1. This is consistent with the Quanta Computer and Apple scenario, and a possibility explored in more detail in the next section.

## 4 HUB AND SPOKE EXAMPLE

While the topology of supply chain networks is highly variable, there is evidence that many networks have a general hub and spoke structure. [35, 36]. In applying our results we focus on an 'idealized' hub and spoke network with firm 1 in the centre and $n-1$ firms in the periphery. For instance, we can envisage a car manufacturer with a number of direct suppliers. The network is summarised in Figure 2 and by the following adjacency matrix, where $b < 1/(n-1)$ is a scalar

$$A = \begin{pmatrix} 0 & b & b & b & \dots & b \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \dots & & & & & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{3}$$

We also assume that the output vector is $V = [Q, q, ..., q]$ where $Q > q > 0$ are parameters. Thus, firm 1 produces a larger output than those firms supplying firm 1.

To illustrate Theorems 3.1 and 3.2 we work through some specific scenarios. First, suppose that the criminals target firm 1 and there is cyber-attack $K = [k_1, 0, ..., 0]$. Applying Theorem 3.2 the optimal ransom from the criminals perspective is $Qk_1$. This is the standard type of ransomware attack studied in the literature. Next suppose that the criminals target firm 2 and there is cyber-attack $K = [0, k_2, ..., 0]$. This has direct effect $c_2 = k_2$ on firm 2 and $c_1 = bk_2$ on firm 1. Applying Theorem 3.1, the optimal ransom to ask firm 1 would be $bk_2Q$ and that to ask firm 2 would be $k_2q$. If the criminals expect the firms to not coordinate ransomware payments then it would be optimal to target firm 1 if $bQ > q$ and firm 2 otherwise.

We can now compare the incentive of the criminals to target the hub, firm 1, or spoke, firm 2. Suppose that the criminals can implement cyber-attack $K^1 = [k_1, 0, ..., 0]$ or $K^2 = [0, k_2, ..., 0]$ for equal cost (or equal likelihood of success). Moreover, suppose they plan to target firm 1 for a ransom (because $bQ > q$). Then it would be optimal for the criminals to choose cyber-attack $K^2$ if $bk_2 > k_1$. This scenario captures the Quanta Computing and Apple example, in which Quanta Computing was attacked and Apple became involved in the ransom demand [17]. Such a scenario is likely if it is relatively difficult to attack the hub (so the disruption from any breach $k_1$ is small) and easier to attack the spoke (so disruption $k_2$ is large).

Just Accepted

The preceding discussion brings us onto the crucial question of whether our analysis can inform on defence against ransomware. Our results show very clearly the need for firms to evaluate the security of their entire supply chain. In particular, if the hub is vulnerable to ransom because of an attack on the spoke then it is in the interests of the hub to invest in the security of firms in the spoke. For instance, returning to the example, it is in the interests of firm 1 to lower the attack on firm 2 as given by $k_2$. Indeed, firm 1 should be willing to invest up to $Q(bk_2 - k_1)$ to improve the cyber security of firm 2 to the point where firm 2 is less vulnerable than firm 1. Put differently, it makes sense for firm 1 to prioritise the security of firm 2 because this is where firm 1 is vulnerable. The same logic applies to firms 3, .., $n$. We see, therefore, that cyber-risk management should apply across the supply chain and not just within a particular firm.

Another consideration is whether the network structure can be changed to lessen the potential impact of a ransomware attack. In our example we considered that firm 1 may be vulnerable to an attack on firm 2 because $bk_2 > k_1$. Thus, as well as decreasing $k_2$, firm 1 could also explore decreasing $b$. In other words, firm 1 could become less reliant on firm 2. In a general sense, it will impose costs on firm 1 to reduce its supply from firm 2 because the supply chain is in place to facilitate efficiency in production. Diversifying the supply chain could, however, be beneficial. For instance, if firm 1 increases the number of suppliers then it can reduce, $b$, its reliance on any one firm. For this to work, however, it is vital that suppliers have independent cyber security systems otherwise a breach in one supplier could be replicated across other suppliers. It is also in the interests of suppliers to be independently cyber-secure if this lowers the risk to firm 1 and, thus, the willingness to firm 1 to rely on them as a supplier. Diversification in supply chain should, therefore, be accompanied by diversification in IT systems.

## 5 SIMULATION ANALYSIS

In this section we generalise the discussion beyond the hub and spoke scenario and explore the optimal ransom strategy of the criminals as a function of characteristics of the supply network. We adopt a simulation approach in which we randomly generate a network and an attack, we identify the relevant characteristics of the resulting network, and calculate the optimal ransom strategy. This allows us to visualise the relationship between the optimal strategy and the supply network.

In the simulations we keep $n = 5$ fixed meaning there are five firms. We also fix $\overline{A} = \sum_{i,j} a_{ij} = 1$, as a baseline for comparison, meaning the total supply inter-dependence is held constant at 1. For comparison we also provide results using $\overline{A} = 0.5$, meaning less inter-dependence, and $\overline{A} = 2$, meaning higher interdependence. To generate a network we randomly assign a supply link from firm $j$ to firm $i$ with probability 0.5. This is repeated, independently, for each pair of firms $j$ and $i$ subject to the network being connected and acyclic. We then reweight connections to satisfy the restriction on $\overline{A}$. Throughout, without loss if generality, firm 1 is a central firm who does not supply another firm in the network, and firm 5 is a periphery firm that does not take supplies from another firm in the network.

The main network characteristic we will focus on in our analysis is the average path length from firms 2, 3, 4 and 5 to firm 1. The smaller the average path length the more suppliers feed directly into firm 1. For instance, the hub and spoke supply network (see Figure 2) has an average path length of 1 with suppliers feeding directly into firm 1. At the other extreme is a supply chain/line, in which firm 5 supplies firm 4, which supplies firm 3, etc. This has the maximal average path length of 2.5. As a final example, the network in Figure 1 has average path length of 1.5.

We considered three methods for randomly generating an attack vector $K = [k_1, ..., k_5]$. First, we consider the case in which each $k_i$ is independently and uniformly drawn from the unit interval, and then normalised so $\sum_i k_i = 1$. Thus, each firm is directly impacted by the attack, with different firms being impacted to different degrees, and the total direct impact is 1. Second, we consider the case in which $k = i = 0.2$ for all $i$. Thus, each

Just Accepted

firm is directly impacted by the same amount. This could reflect overlapping IT systems that mean a breach at one firm allows a breach throughout the supply chain. Finally, we consider the case where one randomly chosen firm suffers a full breach and the other firms experience no direct disruption. Thus, $k_i = 1$ for one firm $i$. Our findings are similar across all three methods of generating an attack vector and so, for the sake of brevity, we focus here on the first scenario in which each $k_i$ is independently drawn.

We summarise the results in Figure 3. In panel (a) of the figure we detail the optimal total ransom, given by Theorem 3.1, in which multiple firms are simultaneously ransomed. You can see that the total ransom is increasing in average path length. Thus, the ransom amount is lowest for a hub and spoke network and highest for a chain/line network. In panel (b) of Figure 3 we detail the optimal ransom, given by Theorem 3.2, if only one firm is ransomed. Thus, the ransom amount is highest for a hub and spoke network and lowest for a chain/line network. We observe, therefore, an interesting contrast: if the criminals can ransom multiple firms in the supply network then they do best from a chain/line network, but if they can only ransom one firm they do best from a hub and spoke network.

The explanation for this result becomes apparent from considering the other panels in Figure 3. Here we plot the optimal ransom for firm 1 (panel c), the average optimal ransom for firms 2, 3 and 4 (d) and the proportion of times it is optimal to ransom firm 1 rather than firms 2 to 5 (e).[3] The optimal ransom for firm 1 is decreasing with average path length while that of firms 2, 3 and 4 is increasing in average path length. Moreover, given its centrality, the optimal ransom for firm 1 is typically higher than that of other firms. Thus, if the criminals can only ransom one firm it is better, from their perspective, to target a hub and spoke network in which they can ransom firm 1. If, however, they can ransom multiple firms then it is better to target a chain/line network in which all five firms can be ransomed.

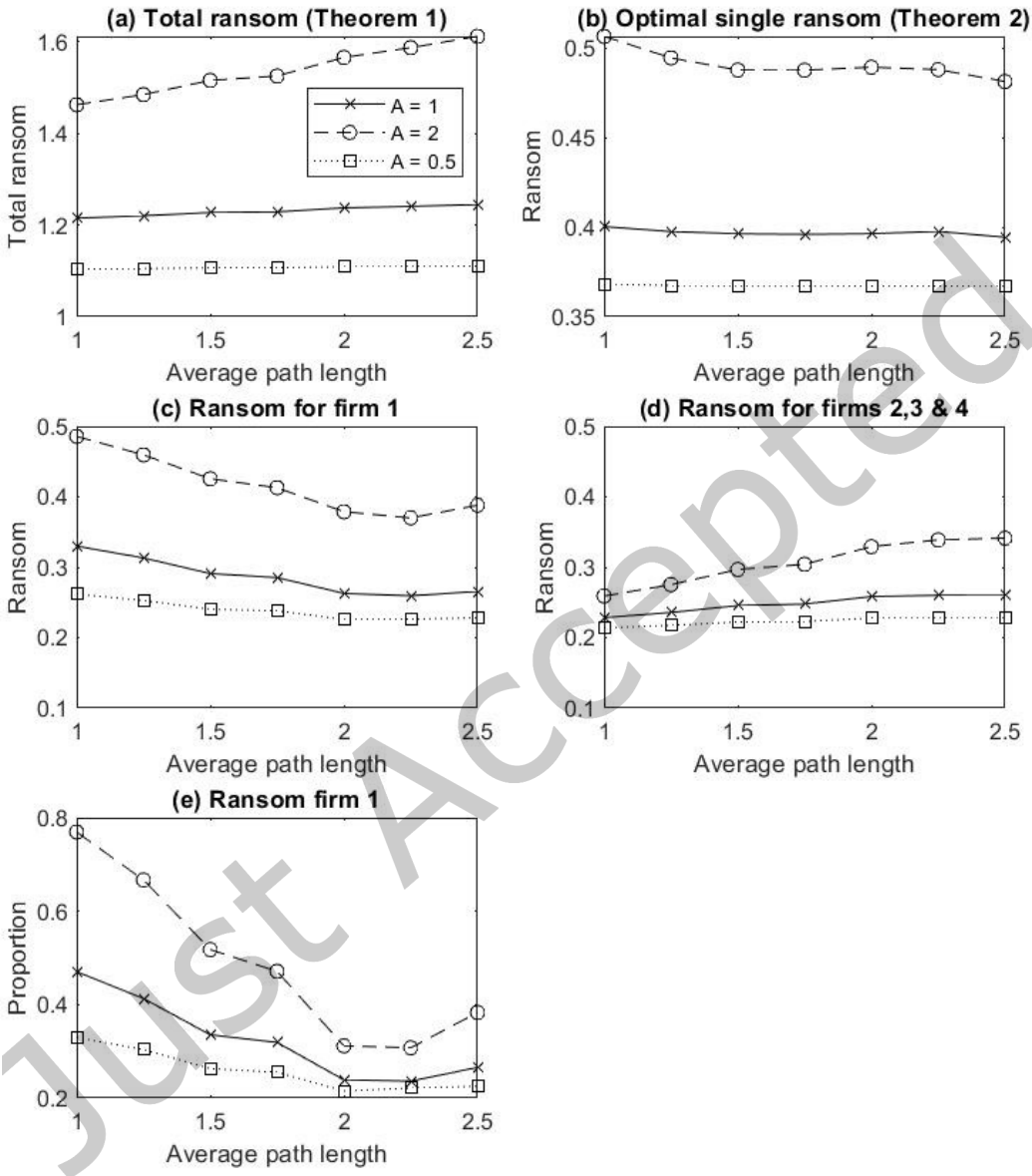
In terms of informing the defence against ransomware the findings in panel (e) are particularly interesting. As one would expect, given its centrality, firm 1 is typically the most lucrative firm for criminals to ransom.[4] This does not necessarily mean the criminals would breach firm 1 because, as we considered in Section 4, firm 1 may be more costly to breach. It more means that, given a breach of the supply chain, it is optimal for the criminals to ransom firm 1. Interestingly, however, as the average path length increases, the incentives for the criminals to ransom firm 1 (rather the one of the other four firms) diminish considerably. From the point of view of firm 1 a hub and spoke network exposes them, therefore, to heightened ransomware risk. On the flip side, firms 2, 3, 4 and 5 are less at risk when on the periphery of a hub and spoke network. This shows that we should not expect 'simple solutions' in terms of determining which network structures are more or less desirable. The focus should, thus, be on understanding the different risk profiles that result from different network structures. We find that suppliers are more at risk the longer the supply chain.

## 6 CONCLUSION

In this paper we have provided a game theoretic analysis of ransomware on supply chain networks. We have demonstrated that new strategies open up to the criminals, such as attacking one firm to ransom another, or simultaneously ransoming multiple firms. Some may question whether such possibilities are destined to remain theoretical possibilities. The recent evolution of ransomware on supply chains suggests not [17, 49]. Ransomware criminals have shown a ready willingness to refine their strategies in search of increased revenue. And the notion that a major manufacturer could be ransomed because of disruption in their supply chain does not seem at all unrealistic. Indeed, attacks on logistics firms and manufacturing supply chains are on the rise [25]. The possibility of criminals exploiting supply chains needs, therefore, to be taken seriously.

[3]The optimal ransom of firm 5 is given by the direct impact and equals (on average) 0.2 and does not depend on network structure.
[4]There are 5 firms and so the baseline proportion for comparison is 0.2.

Just Accepted




Just Accepted

Fig. 3. Optimal criminal strategy as a function of average path length

Our model offers insight on possible defence strategies. Indeed, we identify two key considerations for defence: (i) Supply chains need to be viewed holistically and not piecemeal when defending against cyber-attacks [10, 45]. This needs to go beyond a firm merely taking an interest in the cyber security of suppliers. In particular, it could involve a firm actively investing in the cyber security of suppliers. Such investment makes financial sense if it protects the firm from a ransomware attack through weaknesses in the supply chain. Recent ransomware attacks affecting Apple, Toyota and JSB illustrate the dangers of not investing in the supply chain security [4, 49]. (ii) The supply network can be designed to increase resilience to ransomware attack. There is a large literature on network resilience that can potentially inform on optimal network design [26]. One clear implication from our model is to diversify and decouple risks on the supply chain. This can limit the damage that any one cyber-breach can cause.

The ransomware model of the cyber criminals is undermined if victims do not pay ransoms. In our model we solve for the maximum ransom that criminals could expect victims to be willing to pay. This is a starting point for exploring policy interventions that can combat ransomware. In particular, an objective of policy, both for firms in a supply chain and governments, should be to lower the amount victims are willing to pay. Generally speaking, effective ways to do this include effective back-up procedures and compartmentalisation of security. In our model we see that the maximum ransom is reduced if firms in the supply chain are unable, or expected to be unable, to coordinate with each other in paying a ransom demand. Intuitively, firms in a supply chain would presumably want to be able to coordinate, and so there is something of a paradox. One route out of this paradox could be legal and/or contractual pre-commitments that rule out cross-subsidy ransom payments. For instance, a firm could pre-commit to not paying a ransom if a supplier is attacked. This would lessen the incentive for criminals. The additional liability exposure for suppliers could be offset by cyber security support that increases resilience.

A related factor to consider is cyber insurance. The appropriate division of responsibilities for business disruption caused by an attack on a supply chain are not obvious. Consider, for instance, a cyber attack on one firm which causes disruption to firms further down the chain. The liability for this disruption could spread across multiple firms and insurers. One possibility is to couple insurance across a supply chain. For instance, the central firm, with largest output, could insure its overall supply chain. This, however, suggests the firms in the supply chain could more easily coordinate on a large ransom payment. It may, thus, incentivize attacks. Future work could explore the optimal liability and contract design for secure supply chain networks. One crucial consideration should be for firms in a supply chain to have an agreed, cross network, incident response plan in place that includes, where relevant, provision for negotiating and resolving any ransom demands. In short, ransomware attacks on supply chains are a reality in the modern environment and can have profound implications across the chain, so an agreed resilience policy should be agreed before an attack hits.

Just Accepted

## ACKNOWLEDGMENTS

We would like to thank the three anonymous reviewers for their constructive comments which allowed us to significantly improve the paper. This work was partly supported by A RISCS Fellowship in Quantification and Cyber Risk for A. Cartwright.

## REFERENCES

[1] Christine Abely. 2022. Ransomware, Cyber Sanctions, and the Problem of Timing. *BCL Rev. E. Supp. I-* 63 (2022), 47.

[2] Helen Sydney Adams. 2022. *Why manufacturing supply chains are at risk of cyberattacks. Manufacturing.* Retrieved February 8, 2023 from https://manufacturingdigital.com/procurement-and-supply-chain/why-manufacturing-supply-chains-are-at-risk-of-cyberattacks

[3] Sana Aurangzeb, Muhammad Aleem, Muhammad Azhar Iqbal, Muhammad Arshad Islam, et al. 2017. Ransomware: a survey and trends. *Journal of Information Assurance & Security* 6, 2 (2017), 48–58.

[4] Joshua Becker. 2021. *Cyber attacks on rise as criminals target Australian agricultural supply chains. ABC News.* Retrieved February 8, 2023 from https://www.abc.net.au/news/rural/2021-06-04/cyber-attacks-on-rise-in-agriculture-industry/100188712

[5] Hugh Boyes. 2015. Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review* 5, 4 (2015), 28–34.

[6] Sandor Boyson. 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* 34, 7 (2014), 342–353.

[7] Nicholas Caporusso, Singhtararaksme Chea, and Raied Abukhaled. 2019. A game-theoretical model of ransomware. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9*. Springer, 69–78.

[8] Anna Cartwright and Edward Cartwright. 2019. Ransomware and reputation. *Games* 10, 2 (2019), 26.

[9] Edward Cartwright, Julio Hernandez Castro, and Anna Cartwright. 2019. To pay or not: game theoretic models of ransomware. *Journal of Cybersecurity* 5, 1 (2019), tyz009.

[10] Claudia Colicchia, Alessandro Creazza, and David A Menachof. 2019. Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal* 24, 2 (2019), 215–240.

[11] Lena Y Connolly and David S Wall. 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security* 87 (2019), 101568.

[12] Patrizia Daniele and Shivani Shukla. 2017. A Supply Chain Network Game Theory Model of Cybersecurity Investments with Nonlinear Budget Constraints Anna Nagurney Isenberg School of Management. *Annals of Operations Research* 248, 1 (2017), 405–427.

[13] Giovanna Devetag and Andreas Ortmann. 2007. When and why? A critical survey on coordination failure in the laboratory. *Experimental economics* 10 (2007), 331–344.

[14] Debabrata Dey and Atanu Lahiri. 2021. Should we outlaw ransomware payments? *Proceedings of the 54th Hawaii International Conference on System Sciences* (2021). Retrieved February 8, 2023 from http://hdl.handle.net/10125/71414

[15] Cath Everett. 2016. Ransomware: to pay or not to pay? *Computer Fraud & Security* 2016, 4 (2016), 8–12.

[16] Rui Fang, Maochao Xu, and Peng Zhao. 2020. Should the ransomware be paid? *arXiv preprint arXiv:2010.06700* (2020).

[17] Anthony M. Freed. 2021. *REvil/Sodinokibi ransomware gang extorts Apple through supply chain attack. Cybereason.* Retrieved February 8, 2023 from https://www.cybereason.com/blog/sodinokibi-ransomware-gang-extorts-apple-through-supply-chain-attack

[18] Drew Fudenberg and Jean Tirole. 1991. *Game theory*. MIT press.

[19] Abhijeet Ghadge, Maximilian Weiß, Nigel D Caldwell, and Richard Wilding. 2020. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal* 25, 2 (2020), 223–240.

[20] Pepijn Hack and Zong-Yu Wu. 2021. "We wait, because we know you." Inside the ransomware negotiation economics. *NCC Group, Nov* 12 (2021). https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/

[21] Emily A Heath, John E Mitchell, and Thomas C Sharkey. 2020. Models for restoration decision making for a supply chain network after a cyber attack. *The Journal of Defense Modeling and Simulation* 17, 1 (2020), 5–19.

[22] Julio Hernandez-Castro, Anna Cartwright, and Edward Cartwright. 2020. An economic analysis of ransomware and its welfare consequences. *Royal Society open science* 7, 3 (2020), 190023.

[23] Jon Hoeksma. 2017. NHS cyberattack may prove to be a valuable wake up call. *BMJ* 357 (2017).

[24] Tom Hofmann. 2020. How organisations can ethically negotiate ransomware payments. *Network Security* 2020, 10 (2020), 13–17.

[25] IBM. 2022. *X-Force Threat Intelligence Index 2022*. IBM Report. IBM. https://www.ibm.com/downloads/cas/ADLMYLAZ

[26] Dmitry Ivanov et al. 2018. *Structural dynamics and resilience in supply chain risk management*. Vol. 265. Springer.

[27] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139, 3 (2021), 719–749.

[28] Marc Knez and Colin Camerer. 1994. Creating expectational assets in the laboratory: Coordination in 'weakest-link'games. *Strategic Management Journal* 15, S1 (1994), 101–119.

[29] Aron Laszka, Sadegh Farhang, and Jens Grossklags. 2017. On the economics of ransomware. In *Decision and Game Theory for Security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017, Proceedings*. Springer, 397–417.

[30] Gregory Levitin and Kjell Hausken. 2012. Review of systems defense and attack models. *International Journal of Performability Engineering* 8, 4 (2012), 355.

[31] Yuhong Li, Christopher W Zobel, Onur Seref, and Dean Chatfield. 2020. Network characteristics and supply chain resilience under conditions of risk propagation. *International Journal of Production Economics* 223 (2020), 107529.

[32] Zhen Li and Qi Liao. 2020. Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling ransomware. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 1–9.

[33] Steve Mansfield-Devine. 2016. Ransomware: taking businesses hostage. *Network Security* 2016, 10 (2016), 8–17.

[34] Alessandro Nicita, Victor Ognivtsev, Miho Shirotori, et al. 2013. *Global supply chains: Trade and economic policies for developing countries*. UN.

[35] Supun Perera, H Niles Perera, and Dharshana Kasthurirathna. 2017. Structural characteristics of complex supply chain networks. In *2017 Moratuwa Engineering Research Conference (MERCon)*. IEEE, 135–140.

[36] Supun S Perera, Michael GH Bell, Mahendrarajah Piraveenan, Dharshana Kasthurirathna, and Mamata Parhi. 2018. Topological structure of manufacturing industry supply chain networks. *Complexity* 2018 (2018).


Just Accepted

[37] Timothy J Pettit, Keely L Croxton, and Joseph Fiksel. 2019. The evolution of resilience in supply chain management: a retrospective on ensuring supply chain resilience. *Journal of Business Logistics* 40, 1 (2019), 56–65.
[38] Timothy J Pettit, Joseph Fiksel, and Keely L Croxton. 2010. Ensuring supply chain resilience: development of a conceptual framework. *Journal of business logistics* 31, 1 (2010), 1–21.
[39] Proofpoint. 2022. *2022 State of the Phish.* Proofpoint Report. https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish
[40] TR Reshmi. 2021. Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights* 1, 2 (2021), 100013.
[41] Anna Ribeiro. 2021. *One year after SolarWinds attack, more needs to be done to boost cybersecurity in industrial sector. Industrial Cyber.* Retrieved February, 9, 2023 from https://industrialcyber.co/critical-infrastructure/one-year-after-solarwinds-attack-more-needs-to-be-done-to-boost-cybersecurity-in-industrial-sector/
[42] Ronny Richardson and Max M North. 2017. Ransomware: Evolution, mitigation and prevention. *International Management Review* 13, 1 (2017), 10.
[43] Ronny Richardson, Max M North, and David Garofalo. 2021. Ransomware: The landscape is shifting-a concise report. *International Management Review* 17, 1 (2021), 5–86.
[44] Amy Robinson, Casey Corcoran, and James Waldo. 2022. New Risks in Ransomware: Supply Chain Attacks and Cryptocurrency. *Science, Technology, and Public Policy Program Reports* (2022).
[45] Jay Simon and Ayman Omar. 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research* 282, 1 (2020), 161–171.
[46] Arkadii Snihurov, Oleksandr Shulhin, and Vitaly Balashov. 2018. Experimental studies of ransomware for developing cybersecurity measures. In *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T).* IEEE, 691–695.
[47] Göran Svensson. 2000. A conceptual framework for the analysis of vulnerability in supply chains. *International journal of physical distribution & logistics management.* 30, 9 (2000), 731–750.
[48] Ke Jing Jie He Tang, Liang and H. Eugene Stanley. 2016. Complex interdependent supply chain networks: Cascading failure and robustness. *Physica A: Statistical Mechanics and its Applications.* 443 (2016), 58–69.
[49] Joel Witts. 2021. *The Apple ransomware attack: Supply chains under siege.* Retrieved February, 9, 2023 from https://expertinsights.com/insights/the-apple-ransomware-attack-supply-chains-are-under-siege/
[50] Emma Woollacott. 2022. *Ransomware attacks on the shipping, logistics organizations rising as coronavirus vaccine supply chain targeted.* Retrieved February, 9, 2023 from Ransomwareattacksontheshipping,logisticsorganizationsrisingascoronavirusvaccinesupplychaintargeted.
[51] Lena Yuryna Connolly, David S Wall, Michael Lang, and Bruce Oddson. 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* 6, 1 (2020), tyaa023.
[52] Zhaoshun Wang Zimba, Aaron and Mumbi Chishimba. 2019. Addressing crypto-ransomware attacks: before you decide whether to-pay or not-to. *Journal of Computer Information Systems* (2019).

Just Accepted