
16

INTERDEPENDENT SECURITY IN INTERCONNECTED NETWORKS

*Geoffrey Heal, Michael Kearns, Paul Kleindorfer,
and Howard Kunreuther*

In an interdependent world, the risks faced by any individual, firm, region, or country depend not only on its own choices but also on those of others. In the context of terrorism, the risks faced by any airline, for example, are tied to the security standards of other carriers and airports.

To illustrate this point, consider the destruction of Pan Am flight 103 in 1988. In Malta, terrorists checked a bag containing a bomb on Malta Airlines, which had minimal security procedures. The bag was transferred in Frankfurt to a Pan Am feeder line and then loaded onto Pan Am 103 in London's Heathrow Airport. The transferred piece of luggage was not inspected at either Frankfurt or London – the assumption in each subsequent airport being that baggage had been inspected at the point of origin. The bomb had been designed to explode above 28,000 feet, a height normally attained only on the transatlantic route. The bomb exploded over Lockerbie, Scotland, killing 259 passengers and crew, and another 11 people on the ground. Failures in a peripheral part of the airline network, Malta, compromised the security of a flight leaving from a core hub, London.

A great deal of work on the vulnerability of critical infrastructures to terrorist attacks is described elsewhere in this book. These other chapters focus on individual firms or systems, such as the electric grid, telecommunications services, and the cyber network, and ask how much their security depends on the actions of others due to the transmission of harmful effects from one agent to another (which from now on we refer to as contamination). The analytical framework related to interdependency of the participants in a risk-exposed

Support from NSF grant number CMS-0527598 and the Wharton Risk Management and Decision Processes Center is gratefully acknowledged.

network has important implications for public policies intended to motivate private investment in reducing vulnerability of the system as a whole.

Interdependence does not require proximity. Hence the antecedents to catastrophes can be quite distinct and distant from the actual disaster, as in the case of the September 11, 2001, attacks on the World Trade Center and the Pentagon, when security failures at Boston's Logan airport led to crashes in New York City, Arlington, Virginia, and rural Pennsylvania. The same was true in the case of the August 2003 power failures in the northeastern United States and Canada, where the initiating event occurred in Ohio, but the worst consequences were felt hundreds of miles away. Similarly, a disease in one region can readily spread to other areas, as was the case with the rapid spread of SARS from China to its trading partners.

Two studies by Kunreuther and Heal introduced the concept of "interdependent security" using game-theory models to investigate how the optimal decision of one unit in a system regarding how much to invest in security depends on what others in the system do.¹ More specifically, the interdependent security paradigm raises the following question: To what extent will one agent (e.g., an individual, an organization, a division in a firm) invest in protection, when it is connected to and dependent on others whose failures may compromise its own operations, as the failure at Malta airport compromised security at London airport and led to the crash of PanAm flight 103?

Two characteristics of these interdependent security problems underlie the incentives that organizations face in their efforts to reduce their risk exposure. One is that the risky event occurs only once, and the second that the risk facing one agent is determined in part by the behavior of others. In the equilibria that arise in these problems, it is possible that a change in the behavior of one agent could tip the system from one equilibrium to another.² A related phenomenon is "cascading" – in which a change by one agent leads to a change by a second, which provokes a change by a third, and so on.³

IMPACT OF CONTAMINATION FOR INTERDEPENDENT NETWORKS

The challenges of managing risks within interdependent networks are faced by firms throughout those networks – for example, firms in a computer network, a power grid, or a supply chain. The firms must develop appropriate strategies for reducing risks in a cost-effective manner. If each firm wants to maximize the expected returns from its resources, each needs to determine whether to invest in a risk-mitigation measure such as reducing the likelihood of losses from a

terrorist attack. When the firms are interdependent, each has less incentive to invest in protective measures if the others have not taken similar action.

To illustrate this point, consider two firms, DataCollate and InfoAware. Each firm faces a certain probability of a terrorist attack that damages itself, and another probability that such an attack on itself disrupts the activities of the other firm due to interdependencies through a network. Suppose DataCollate invests in security measures, and by so doing avoids incurring an attack on its own firm. If, however, InfoAware does not invest in its own security, DataCollate faces an additional risk that it will be harmed by an attack at InfoAware. More specifically, even if DataCollate invests in security measures, there is still a probability that InfoAware will be attacked, in which case DataCollate also incurs a loss (and this loss comes at a cost in addition to the amount it has already paid for its own security measures). This possibility reduces the incentive for DataCollate to invest in protection. Why? Because investing in security buys less protection when there is the possibility of contamination from others due to interdependencies. (Appendix 16.A presents a more formal analysis of this interdependent security problem for the case of two firms.)

The results for the two-firm interdependent security case carry over to more general settings with some increase in complexity. The incentive for any firm to invest in protection depends on how many other firms there are and on whether these other firms are investing. Other firms that do not invest in security reduce the expected benefits from one's own protective actions and hence reduce a firm's incentive to invest.

If there are many identical firms, and all firms invest in security, then the probability that any firm will experience a loss will be low. If, however, no firm invests in security (and assuming that these firms can contaminate the others), then the likelihood of a loss to any firm in the network increases. Therefore, the greater the number of unprotected firms, the lower the incentive for any firm to invest in protecting itself against a catastrophe.

Intuitively, this result is due to interactions of weak links on others in the system. One unprotected firm endangers all of the other firms, even if they have invested in security. As more firms decide not to invest in security, the probability of a failure in the system increases and the economic incentive for any specific firm to undertake protection decreases. As the number of firms gets large, this probability approaches 1, and a firm will not be willing to incur any costs to invest in security because it knows it will be contaminated by one or more of the many unprotected firms.

TIPPING AND CASCADING BEHAVIOR

The fact that significant negative externalities are imposed by some firms on others in an interdependent security context is both a curse and a blessing.

The curse derives from the scenario noted above; the blessing may come about through leveraging reduced externalities to induce phenomena known as tipping and cascading, in which one firm after the next finds it in its interest to invest in protective behavior because others are taking such actions. There may be ways of inducing tipping and cascading so that everyone's welfare is improved. If firms are heterogeneous (so that they have different risks and costs associated with their activities), some firms in the previous example may have much higher risks than others of a large-scale accident that has system-wide implications.

Heal and Kunreuther show that one firm may occupy such a strategic position that if it changes from not investing to investing in protection, then all others will find it in their interests to follow suit.⁴ Even if no single firm can exert such leverage, a small group may be able to do so. More specifically, the firm that would create the largest negative externalities for others in the system should be encouraged to invest in protective behavior, not only to reduce its own losses but also to induce other firms to follow suit.

This type of tipping behavior is in the spirit of the many interesting examples described by Schelling, where one equilibrium suddenly changes to another due to the movement of a few agents (e.g., the sudden change in the racial composition of a neighborhood).⁵ Tipping and cascading behavior implies that one needs to focus on only certain key parts of a system to convince others to follow suit. This behavior suggests the particular importance of persuading some key players to manage risks more carefully. Working with them may be a substitute for working with all firms.

APPLICATIONS TO SUPPLY CHAIN MANAGEMENT

Interdependencies exist across supply chains in every industry, and the complexity of these interdependencies has been growing by leaps and bounds as industry has become more globalized through outsourcing and off-shoring activities. The result is that global supply chains that source from one country for manufacturing or retailing operations in another now dominate many of the major economic sectors, from the automotive industry to semiconductors to the huge retail industry represented by giants like Wal-Mart and Home Depot.

The increased complexity of such global supply chains has added levels of risk and interdependence that are sometimes not evident until disaster strikes, exposing hidden vulnerabilities and leading to large economic losses. The Taiwan earthquake of September 1999, which sent shock waves through the global semiconductor market,⁶ the 9/11 terrorist attack on the World Trade Center, and the August 2003 blackout in the northeastern United States and

Canada are but a few recent reminders of the potential for significant disruptions to supply chains. More recently, hurricanes Katrina and Rita in 2005 have led to huge disruptions in economic and business activity in the affected states, which are likely to far outstrip the significant property losses of these events. Interestingly, the Taiwan earthquake was largely seen as a business disruption, with responsibility for recovery falling on the business community, while hurricanes Katrina and Rita were seen for their effects on human suffering, with the government responsible for response and recovery. Whatever the perceptions of these events, the fact is that firms that are better prepared for such supply chain disruptions are increasingly being favored in the market place as better economic risks. We consider first the evidence for this claim, and then note the challenges presented in managing interdependent security problems across such supply chains.

The effects of supply chain disruptions (whether from natural disasters, terrorists, or other unexpected events) on the profitability of supply chain participants are now recognized as being potentially very large. Hendricks and Singhal analyze announced shipping delays and other supply chain disruptions reported in the *Wall Street Journal* during the 1990s and show that companies experiencing such disruptions under-perform their peers significantly in stock market performance as well as in operating performance, as reflected in costs, sales, and profits.⁷ Coping with the management challenges of such disruptions is, however, a very difficult matter, as the interdependencies involved require cooperative activity and monitoring across the supply chain in ways that are not captured in the traditional intra-supply-chain metrics of price, cycle time, and product quality. To comprehend the problem, it is necessary to understand the background underlying supply chain management as it has evolved in the recent period of increasing globalization.

Supply chain management has grown steadily in importance over the past two decades.⁸ First came the “just-in-time revolution” in the 1980s, which led to increased efficiency, both internal to companies and between companies and their suppliers and customers. The just-in-time revolution led directly to the recognition of a host of hidden costs associated with supplier and customer relationships, and it resulted in further initiatives in the early 1990s for companies around the world to re-engineer and rationalize procurement functions and interfaces with customers. With the continuing liberalization of international trade, and the associated emergence of China and India as important manufacturing sources, companies around the world looked increasingly to outsourcing and off-shoring activities for sourcing labor-intensive manufactured goods.

The effect of all of these trends has been the globalization of supply chains and head-to-head competition among manufacturing and raw material sources across the planet. The resulting supply chains are considerably more

complicated than their earlier cousins of a few decades back because of their length and their multi-national character. Moreover, these same supply chains are under constant pressure to become leaner, with less inventory and less redundancy. These trends, visible from commodity metals to semiconductors to textiles, imply both increasing efficiency of supply chains and increasing vulnerability of such supply chains to disruptions. Longer paths and shorter clock speeds imply more opportunities for disruption and a smaller margin for error if a disruption takes place.

There are many sources of potential disruption to global supply chains, some of them just from pure congestion in ports and other (de-)consolidation centers. Today security and concerns with global terrorism have become central drivers of senior management concerns for disruption management of global supply chains, partly because of the sinister and unpredictable character of terrorism that makes traditional financial and operational response strategies less effective against it. These underlying reasons, together with the increasing evidence of the profit impact of good disruption risk management noted above, have made security of global supply chains and multi-modal logistics systems an important focus of supply chain disruption management.

Effective management strategies for security in global supply chains cannot be specific to one company. Rather, these strategies need to encompass the entire supply chain of all the organizations participating in the supply chain. But one cannot stop there either, because much of the infrastructure, such as ports and (de-)consolidation centers, serves multiple organizations, including end users and shippers, some in private hands and some under government control. To deal with the security problem, a broad private and public partnership is required. One public-private partnership, launched between the container traffic industry and the retail industry, is effectively dealing with the interdependent security problems in global retail supply chains.

THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM APPROACH

Spurred by the new U.S. Department of Homeland Security's (DHS's) assessment of needs for protection of critical infrastructure, major retailers and the transportation and logistic specialists that provided shipping services to them were brought together in 2002 to discuss the requirements and responsibilities that the private and public sectors should respectively bear in meeting the new challenges of interdependent security in global supply chains. The key objective of both the private and public sectors in these early discussions was to determine the partnership principles to guide the development of standards and certification procedures for improved security for these companies. Major retailers involved in container-based trade (such as Wal-Mart and Home Depot)

recognized the primacy of developing a joint solution that assured continued facilitation of international trade with a high level of security. Major disruptions to any major trans-shipment point, such as a port or (de-)consolidation center, would have significant negative externalities for many retailers, and not just the retailer whose shipment had been the target of a terrorist attack.

These early discussions were eventually synthesized in the United States into a voluntary public-private partnership approach to cargo security that was named Customs-Trade Partnership Against Terrorism (C-TPAT). The principles of C-TPAT were then further elaborated in the National Defense Transportation Agency's Security Best Practices Committee, operating in cooperation with DHS and the Transportation Security Administration. The idea of C-TPAT was to develop basic principles, and associated best practices, for all participants in a global supply chain in four areas: site security, personnel (including background checks), material movements, and process control.⁹ Right from the start, these discussions elicited the idea that large retailers would use their buying power to insist that all elements of their supply chains, beginning with manufacturers, comply with the emerging best practices in these areas. Retailers would also submit to having their compliance audited by the appropriate DHS systems, as well as those of relevant international customs agencies. This tipping strategy has been quite effective in promoting enrollments within the United States; the Customs and Border Patrol noted that, as of November 2004, C-TPAT had more than 7,400 enrolled partners, including 86 of the top 100 U.S. importers by containerized cargo volume. The 7,400 partners cover more than 40 percent of all the imports by dollar value into the United States and more than 96 percent of all the U.S. inbound maritime container carrier traffic.¹⁰

The C-TPAT approach foresees integrating the activities of three types of key actors: (1) private companies that manage supply chains (including manufacturers at the front end and retailers and shippers downstream); (2) port authorities and (de-)consolidators (in the United States and elsewhere) that have the responsibility for clearing cargo and for its loading/unloading; and (3) local, regional, and national agencies (including DHS and the Transportation Security Administration) that have the responsibility for assuring homeland security, including responding to threats and abnormal conditions.

At the company level, the C-TPAT approach to supply chain security management encompasses concerns from the originating manufacturer to the final wholesale and retail outlets. Large companies have developed security metrics (including the scope of integrity of seals, continuous movement of the container, length of time in exposed areas such as foreign ports, and a number of cost metrics) to evaluate approaches to improving global supply chain security. The available methods and technologies for mitigation include certification of

Interdependent Security in Interconnected Networks

Establish voluntary security standard	Assess risk across supply chain	Evaluate, study costs and benefits, and prioritize	Build strategic improvements and public-private partnerships
<ol style="list-style-type: none"> 1. Design voluntary standard for supply chain security management that will allow private firms to achieve reasonable “internal levels” of security 2. Set standards to be compatible with current best industry practices and available technology 3. Coordinate with key private players to achieve “critical mass” to achieve tipping 	<ol style="list-style-type: none"> 1. For each sector (e.g., shippers, consolidators, retailers) determine main assets/processes 2. Assess vulnerabilities of each asset and process 3. Categorize according to level of vulnerability under various scenarios 4. Determine synergies with reduction in theft losses and other key metrics 	<ol style="list-style-type: none"> 1. Develop and validate models for assessing costs and benefits of security-related interventions 2. Value potential damage of a security breach for each asset class: <ul style="list-style-type: none"> • direct/indirect • externalities 3. Prioritize mitigation initiatives for various processes and asset classes 	<ol style="list-style-type: none"> 1. Analyze alternative strategies to reduce risks of security breaches/attacks 2. Evaluate direct and indirect costs of best available actions 3. Analyze alternatives to re-align public and private interests: <ul style="list-style-type: none"> • tax incentives • legal reform • required insurance 4. Design audit system to monitor effectiveness and compliance

Figure 16.1. Security Management in Global Supply Chains.

personnel, audit procedures, and approaches to assuring the integrity (tamper-proofness) of containers. The key to the success of this approach is leveraging those organizations in the global supply chain that have the resources and the information to undertake necessary precautions locally, while assuring that larger problems arising from interdependencies are addressed at the level of the entire supply chain.

Figure 16.1 illustrates the general approach being pursued in the United States for security management in global supply chains. The approach begins with the adoption of a voluntary standard (e.g., in retailing, the principles embodied in C-TPAT and associated relevant metrics for the retail sector). It is envisaged that the adoption of this standard by the major players in global supply chains will lead, via the tipping effect, to widespread adoption of the standard. For those having adopted the standard, best practices are identified along the supply chain, including tracking, monitoring, new technologies, and security metrics. These best practices are further refined in specific companies and sectors and shared among all supply chain participants, which leads to improved private-sector solutions. These solutions are then integrated into evolving public-sector initiatives to yield the desired public-private partnership that will define security management systems and their interfaces with public responders and law enforcement officials, including those at DHS and

its subsidiary organizations (such as the Transportation Security Agency and Customs and Border Control).

In terms of the interdependent security framework described earlier in this chapter, interdependencies are evident in two fundamental areas: (1) in the adoption and implementation of the voluntary standard for security management by each private company in a supply chain, and (2) in the adoption of global standards and technologies across the supply chain. Both of these activities have essential elements of the interdependent security problem embedded in them.

The adoption and implementation of a voluntary standard such as C-TPAT requires more than just lip service to be effective. Personnel screening, vulnerability assessment, and monitoring of material movements throughout the supply chain are required to cope with interdependent security issues. One weak link is enough to allow penetration of a purposeful agent and to undermine the risk mitigation actions of all others in the supply chain.

Improvements to monitoring could contribute to the security of the supply chain. For example, companies could adopt uniform global technology standards, such as radio frequency identification (RFID) technology. RFID technology allows for micro-chips to be installed in each product shipped as well as in pallets and containers. While such technology has considerable potential for enhancing inventory control as well as for contingent responses to terrorist events, it is potentially costly, and the costs may fall unevenly on different supply chain participants. For global retail supply chains, RFID technology requires both significant costs at the originating manufacturer as well as at the final wholesale or retail outlets where such RFID technology would replace barcoding equipment at checkout counters. How such costs would be shared through direct pricing or other funding mechanisms (possibly subsidized by the government) is a thorny problem. It requires that all participants in a supply chain or in a sector agree on a timetable to implement it. The resulting bargaining problem bears a strong resemblance to the interdependent security problem analyzed in Appendix 16.A.¹¹

In addition to adopting specific technologies, other options include implementing information and monitoring programs that would require each participant in a sector or a supply chain to gather, verify, and share certain information on a routine basis. The information could be on security breaches, on facility or company-wide audit results according to specific standards, or on supply chain metrics such as speed of movement through various facilities or other indicators of vulnerability to security breaches. Such information systems would be critical to the risk assessment process for the entire supply chain, and they would help identify weak links where risk mitigation would have the highest payoff.

This sketch of the interdependent security challenges in global supply chains only scratches the surface of the interdependency problems inherent in security management. As predicted by the interdependent security framework, one encounters the expected problems of obtaining compliance across large and small organizations in the same supply chain or sector, given the externalities associated with contamination. Free-rider problems also arise, along with the challenges of inducing tipping and cascading when risks are shared across different units in the system. Added to the complexity is the multi-jurisdictional nature of the problem, which mixes the involvement of private companies, publicly owned ports, and multiple national governments in defining and enforcing the standards that would lead to credible public-private partnerships. Given the importance of international trade (currently estimated by the World Bank to be roughly \$8 trillion and growing), the problem of global supply chain security is likely to remain a major concern for the foreseeable future.

APPLICATIONS TO COMPUTER SECURITY

Another important domain in which interdependent security models seem both appropriate and promising is that of computer network security. The very term “computer virus” highlights the fact that many modern computer security exploits spread in the same manner as do diseases such as SARS: through contacts in a complex (virtual) network of communication. While this epidemiological metaphor has been present in computer security circles for some time now, the game theory aspects of such problems have received less attention, yet they are good targets for interdependent security modeling. The notion of a (relatively) catastrophic event is certainly present, as the most malicious modern computer exploits can effectively destroy important machines, documents, and other resources. However, if an individual’s electronic mail contacts are sufficiently “immunized” against transmitting viruses and worms (for instance, through the diligent application and maintenance of commercial or other anti-virus software), that person may have relatively little incentive to maintain best security practices. If the same contacts are routinely forwarding viruses, the individual has great incentive to immunize. Such an incentive structure can be mapped into the interdependent security framework.

There are also computer security settings in which catastrophic risk has a more collective nature, as an example adapted from Kearns¹² demonstrates. Imagine the user population of a large organization in which each individual has a desktop computer with its own local software and memory, but in which users also maintain important data files or documents on a shared disk drive accessible to the entire organization. From the perspective of the organization,

the primary security concern – the “catastrophic event” in interdependent security parlance – is that an intrusion (whether by a piece of malicious software or a human hacker) might erase the contents of the shared hard drive.

Each user’s desktop computer and its contents – including e-mail, downloaded programs or files, and other components – is a potential point of entry for such intrusion.

Users must at least implicitly decide about many aspects of their individual security practices: how often they change their passwords (and how secure those passwords are against dictionary attacks and other common attacks), whether they enable encryption in their Web and e-mail communications, how careful they are in not downloading suspicious files and programs, whether they maintain their anti-virus software, and many other features. The vulnerability of the shared hard drive is determined by the collective behavior along these dimensions.

If individual users feel quite confident that the overall population is adhering to fairly diligent security practices, their incentive to also be diligent is high, because their negligence would constitute a first-order contribution to the shared disk’s vulnerability. Conversely, if individuals are convinced that their colleagues are lax on security, and if there are many colleagues, this diligence incentive may be sharply reduced – the disk is already so vulnerable from the collective behavior of others in the system that one user’s rigor will have only a marginal impact.

This scenario is just one of many good matches between the original interdependent security model and problems in computer security. Moreover, such matches can drive new research in interdependent security in both theoretical and experimental directions.

SHARED RESOURCES AND PARTIAL CATASTROPHES

One generalization of the basic interdependent security model that arises naturally in many computer security problems involves the complexity and heterogeneity of shared resources. In many interdependent security problems, catastrophes are “private” – for instance, in the airline security problem, individual airline carriers suffer explosions. In the shared disk example above, however, the catastrophe is “public” – the disk’s erasure damages the entire organization. This damage is similar to the problem of supplying power in an integrated network or the global supply chain problem discussed earlier, where there is a weak link in the system.

Computer security overall exhibits many potential problems falling in between the wholly public and wholly private extremes. For example, on many shared computing and file servers, resources may be accessible by only subsets of the population. Thus, a file that is accessible only to one set of users may be

erased by certain breaches of the accounts of those users, but not by breaches of the accounts of other users. Such partially shared resources might arise from organizational structure (e.g., only managers are permitted to read and write to personnel files), informal working groups (e.g., a research team sharing data files), and many other sources. The pattern of subsets of shared resources can be complex indeed on systems of even moderate population size.

In an interdependent security setting, such partially shared resources lead to the notion of a “partial catastrophe.” If the account of user A is breached and all resources accessible to A are destroyed, this is a “full catastrophe” for user A, but it might be one of varying severity for other users, depending on the number and value of resources they share with A.

FUTURE EXPERIMENTS IN COMPUTER NETWORK SECURITY

Another appealing feature of the computer security applications of interdependent security outlined above is the potential for numerical experiments, due to the availability of relevant data. To date, discussion of interdependent security models in the context of specific problems has been largely conceptual and theoretical. The lone exception to this is a numerical model and study in airline security.¹³ This study was handicapped by the unavailability of data pertinent to the estimation of certain parameters in the interdependent security model, which had to be set to default values. In contrast, we believe that much more complete, realistic, and informative experimental interdependent security case studies could be performed in computer security.

In the networks of many organizations, detailed information is routinely logged that could be directly or indirectly used in the derivation of interdependent security models for some of the security scenarios we provide. For example (and setting aside non-trivial privacy issues), to estimate the direct risk parameter associated with a particular user of a system, one could examine the historical record of security flaws or breaches associated with that user’s resources, measure the frequency of his password changes, monitor the rate of virus and worm arrivals in his e-mail, and check the freshness of his anti-virus signatures. Many other measurements are also possible. Similarly, in the “partial catastrophe” scenario described in the previous section, one could directly examine (for instance) file permissions to determine who has a shared stake in each resource. One could even use the time the user takes to edit a document as a measure of the “value” of that document to the user, and incorporate such valuations in to the numerical interdependent security model.

Many interesting and important security questions could be addressed by such detailed numerical interdependent security models. For example, what is the “distribution of vulnerability” across users in a typical or specific organization’s computer network(s)? Building on that, are there a small number of

users whose practices and exposures render them much more vulnerable than the average, or is the vulnerability more evenly spread? Another question might be, given limited resources or budget, what are the best policies for improving the overall level of security of a network? This is related to the first question, as it could dictate (for example) the dramatic improvement of security for a few individuals or incremental increases in security across the entire population.

Such sociological and strategic studies are particularly timely, because the technical computer security community is largely concerned with technological “solutions” or approaches to such problems, and thus less likely to undertake such a line of work.

STRATEGIES FOR REDUCING INTERDEPENDENT SECURITY RISKS

If firms are reluctant to adopt protective measures to reduce the chances of catastrophic losses due to the possibility of contamination from weak links in the system, the private and public sectors may have a role to play in addressing this problem. Strategies will require both structural and communications relationships within the private sector and with government at all levels.

TRADE ASSOCIATIONS AND KEY FIRMS

Leadership from industry, either through trade associations and/or through influential firms that take the lead, can convince others of the need to adopt security measures. A trade association can play a coordinating role by stipulating that any member must follow certain rules and regulations and has the right of refusal if they are asked to do business with an agent that is not a member of the association and/or has not subscribed to the ruling. In the example of baggage security, an airline trade association could require all bags to be reviewed carefully, and each airline could indicate its unwillingness to accept in-transit bags from airlines that do not adhere to this regulation.

Even without a formal mechanism, if a few airlines were to voluntarily undertake these measures they could convince others to follow suit. Kearns and Ortiz use computational algorithms to analyze behavior of airlines with respect to investing in security measures.¹⁴ They analyzed data from 49 major international airlines using airline passenger reservations covering all bookings – including transfers between airlines – in a commercial air reservation system on a single day. Their model suggests that three carriers form a tipping set. These carriers’ decision to invest creates an economic incentive for a large population of otherwise skeptical carriers to follow suit. Kearns and Ortiz’ simulations

suggest that a small group of firms may be able to tip the entire industry from a starting equilibrium in which no one invests in security, to a new equilibrium that improves security and increases expected profits of all firms in the network.

THIRD-PARTY INSPECTIONS, INSURANCE, AND REGULATIONS

There may be a role for governmental standards and regulations coupled with third-party inspections and insurance for enforcement purposes. For example, third-party inspections coupled with insurance protection could encourage decentralized firms in the supply chain to reduce their risks from accidents and disasters. Such a management-based regulatory strategy would shift the locus of decision making from the regulator to individual firms. The firms would then be required to do their own planning as to how they would meet a set of standards or regulations.¹⁵

If these firms take preventive action, they can encourage the remaining ones to comply with the regulations to avoid being caught and fined. This is another form of tipping behavior. Without some type of inspection, low-risk divisions that have adopted risk-reducing measures cannot credibly distinguish themselves from the high-risk ones that have not. By delegating part of the inspection process to the private sector through insurance companies and certified third-party inspectors, regulatory agencies such as DHS can provide a channel through which the low-risk firms can speak for themselves. If a firm chooses not to be inspected by certified third parties, it is more likely to be a high-risk rather than a low-risk one. If a firm does agree to inspection and receives a seal of approval that it is protecting itself against catastrophe, the firm will pay a lower insurance premium than one that does not undertake actions to lower its risk. In this way, regulatory agencies can reduce the number of audits they need to undertake, because they know who has received seals of approval from private third-party inspectors.¹⁶

Third-party inspections complement existing regulatory oversight. DHS, which has limited personnel and funds, has restricted capability to audit for itself all the firms in the supply chain. Without a relatively plausible expectation of inspection, however, firms could not be expected to adopt new behaviors. For example, chemical firms, particularly smaller ones, demonstrate little financial incentive to adopt certain requirements if they perceive that they are unlikely to be inspected and/or they know that the fine is small if they are caught. In such cases, they may be willing to take their chances and risk the financial penalties. The combination of third-party inspections in conjunction with insurance, however, is a powerful duo of private-market mechanisms that can convince many firms of the advantages of implementing security measures to make their operations safer.

OPEN ISSUES

A number of open issues need to be considered when addressing interdependent security issues and the management of risk, including multi-period and dynamic models, behavioral considerations, and endogenous probabilities.

In multi-period and dynamic models, deciding whether to invest in security normally involves multi-period considerations, because the upfront investment cost needs to be compared with the benefits over the life of the protective measure. From the point of view of dynamics, the decision to invest depends on how many others have taken similar actions. How does one start the process of investing in security? Should one subsidize or provide extra benefits to those willing to be innovators in this regard to encourage others to take similar actions?

Regarding behavioral considerations, the interdependent security models to date all assume that individuals make their decisions by comparing their expected benefits (with and without protection) to the costs of investing in security. This is a rational model of behavior. A growing literature in behavioral economics suggests, however, that individuals make choices in ways that differ from the rational model.¹⁷

With respect to protective measures, evidence from controlled field studies and laboratory experiments suggest that many individuals are not willing to invest in protection for a number of reasons that include myopia, high discount rates, and budget constraints.¹⁸ In the models considered in this chapter, no internal positive effects were associated with protective measures. However, many individuals invest in security to gain peace of mind and to relieve anxiety about their perceptions of what might happen to themselves or to others in the event of a security-related incident.

The interdependent security model described previously implicitly assumes that the risks faced by the firms in the network are independent of their own behavior, rather than being endogenous. In reality, if some firms are known to be more security-conscious than others, they are presumably less likely to be terrorist targets. In this sense, investing in security has similarities to theft protection: if a house announces that it has installed an alarm, then burglars are likely to turn to other houses as targets instead.¹⁹ Similarly, in the case of the chemical supply chain, terrorists are more likely to focus on targets that are less well protected.²⁰

For interdependent security problems, a firm is more likely to invest in security when probabilities are endogenous than when these probabilities are exogenous, because of the increased likelihood of being a target when others invest in protection.²¹ Future research should examine how changes in endogenous probabilities affect interdependent security solutions, and the appropriate

strategies for improving the performance of individual firms as well as the security of multiple companies whose security is interdependent with others.

CONCLUSIONS

Our objective in this chapter has been to lay out the logic of interdependent security through a set of examples, notably airline security, global supply chain management, and computer security. The interdependent security model characterizes the nature of the problem facing individual agents as well as the need for public–private partnerships for coping with the negative externalities generated by the linkages between units in the system. Other chapters in this volume point to similar interdependent security effects in areas of critical infrastructure. Indeed, the very character of infrastructure is that of a supporting mechanism for economic agents. Thus, whether in electric power, ports, chemical manufacturing, or the Internet, the value of these major pieces of critical infrastructure systems is their use by multiple organizations and individuals for other economic or social purposes.

The key externalities identified by the interdependent security framework are determined by the nature of the protective actions taken or not taken by others using or having access to the system. This particular characteristic implies that individual decisions regarding risk-reducing measures based on the usual cost–benefit analysis will be influenced in fundamental ways by the behavior of others. In particular, the reliance on pure market solutions that depend solely on individual initiatives may fail in interdependent security environments. Thus coordinative mechanisms are needed through trade associations and sharing best practices across individuals and companies to promote actions that enhance individual and social welfare. Alternatively, private-sector initiatives such as third-party inspections, and insurance can be combined with public sector actions such as well-enforced regulations and standards. The many applications in this book illustrate how such coordinating mechanisms are developing across multiple areas of critical infrastructure.

As the other chapters in this book note, interdependencies and coordination are further exacerbated by the complexity of purposeful agents acting out of complex motivations to do harm. Thus, while the interdependent security framework provides some insights as to the nature of needed strategies and policies to combat this, we still have much to learn about the behavior of agents facing interdependency problems and the impact of firms' actions on developing private–public partnerships for protecting our critical infrastructures.

APPENDIX 16.A. FORMAL GAME THEORETIC ANALYSIS
 OF THE INTERDEPENDENT SECURITY PROBLEM

The Two-Firm Case

Let Y be the assets of each firm before it invests in security or incurs any losses during the year from a terrorist attack. If the firm incurs a cost of c for security, it will be totally protected against a terrorist attack of its own firm but still may be contaminated by the other firm if that firm does not invest in security. Each firm has two choices: invest in security, S , or do not invest, N . A simple 2×2 matrix of the four possible paired outcomes illustrates what happens to the expected returns of each firm as a function of the choices each makes (Table 16.A).

To illustrate the nature of the expected returns, consider the upper left hand box where both firms invest in security (S, S). Then each firm incurs a cost of c and faces no possible catastrophic accidents so that each of their net returns are $Y - c$.

If A_1 invests and A_2 does not, then this outcome is captured in the upper right hand box (S, N). Here A_1 incurs an investment cost of c , but there is still a chance, q_2 , that A_2 will suffer a terrorist attack that will impact A_1 causing a loss of L . This type of contamination imposed by A_2 on A_1 is referred to in economics as a negative externality. A_2 incurs no cost of protecting itself and faces no risk of a loss from A_1 , but it does face the risk of a terrorist attack to its own firm with an expected loss of $p_1 L$. The lower left box (N, S) has payoffs which are just the mirror image of these.

Suppose that neither firm invests in protection (N, N) – the lower right hand box of Table 16.A. Then each firm i has an expected return of $Y - p_i L - (1 - p_i) q_j L$, where j refers to the other firm. The expected losses can be characterized in the following manner. The term $p_i L$ reflects the expected loss originating from an accident in one's own firm i . The second term reflects the expected loss from an attack originating at firm j that contaminates firm i ($q_j L$) and is multiplied by $(1 - p_i)$ to reflect the assumption that a terrorist attack during a given time period can only occur once. In other words, the risk of contamination only matters to a firm when that firm does not have a terrorist attack itself.

Because each firm i wants to maximize its expected returns, the conditions for it to invest in protection against a catastrophic accident are $c < p_i L$ and $c < p_i (1 - q_j) L$. The first constraint is what one would expect if firm i was totally independent of firm j : that is, the cost of investing in protection must be less than the expected cost of a terrorist attack. If firms A_1 and A_2 are independent, this tightens the constraint by reflecting the possibility of contamination from the other firm.

Table 16.A Expected returns associated with investing in security measures (S) and not investing in security (N)

		Firm A_2	
		S	N
Firm A_1	S	$Y - c, Y - c$	$Y - c - q_2 L, Y - p_1 L$
	N	$Y - p_1 L, Y - c - q_1 L$	$Y - [p_1 L + (1 - p_1) q_2 L],$ $Y - [p_2 L + (1 - p_2) q_1 L]$

The Multi-Firm Case

Consider the case in which there are n identical firms. As shown by Kunreuther and Heal,²² if none of the other firms are protected, then the condition for any firm to invest in protection is given by the following condition:

$c < p[L - X(n,0)]$, where $X(n,0)$ represents the negative externalities to the firm if none of the other firms in the system invests in security]. Let c^* be the value of c where the firm is indifferent between investing and not investing in protection when j of the other firms have invested in security: $c^* = p[L - X(n,j)]$. If there are no negative externalities because all the other firms have invested in security, then $c^* = pL$, which is the same as if the firm were operating in isolation. As more firms do not invest in protection, c^* decreases, so that the firm is less likely to take security measures if it is maximizing its expected returns.

NOTES

1. See Kunreuther and Heal 2003 and Heal and Kunreuther 2005a.
2. See Schelling 1978.
3. See Dixit 2002 and Farrell and Saloner 1985.
4. Heal and Kunreuther 2006.
5. Schelling 1978.
6. Papadakis and Ziemba 2001.
7. Hendricks and Singhal 2005.
8. Kleindorfer and Van Wassenhove 2004.
9. See Kleindorfer and Saad 2005 for a discussion of how C-TPAT integrates with other supply chain security and risk management practices.
10. See USCBP 2004.
11. See Heinrich 2005 for a detailed discussion of the costs and benefits of RFID technology for security and other purposes.
12. Kearns 2005.
13. Kearns and Ortiz 2004.
14. Kearns and Ortiz 2004.
15. Coglianese and Lazer 2003.
16. For more details on this approach, see Kunreuther et al. 2002a.
17. See Kahneman and Tversky 2000.
18. For more details, see Kunreuther 2001.
19. Kunreuther and Heal 2003.
20. Keohane and Zeckhauser 2003.
21. Heal and Kunreuther 2005b.
22. Kunreuther and Heal 2003.

