COMPREHENSIVE CYBER SECURITY VULNERABILITY ANALYSIS FOR MANUFACTURING PLANTS

by Paul Baybutt, Primatech Inc.
50 Northwoods Blvd., Columbus, OH 43235
614-841-9800 (T) 614-841-9805 (F)
paulb@primatech.com

A version of this paper appeared in Hydrocarbon Engineering, pps 12 - 18, Vol. 10, No. 1, January 2005.

Abstract

Manufacturing plants use computer systems to control manufacturing processes, store information, and manage value chain activities. All these computer systems can be attacked by cyber means and used to cause harm. Cyber security is an established discipline for information technology (IT) security but not for control systems or the value chain where the risk has only recently been recognized.

Many approaches to IT security use checklist-based assessment methods to identify controls needed to manage cyber security risks. However, such methods are not risk analyses per se. They focus attention on comparing existing controls with an idealized set. Similar approaches are sometimes used in safety analysis. While they play an important role in ensuring that codes and standards are met, they do not provide the means for evaluating novel threat scenarios that are not covered by the codes and standards. This is especially an issue for cyber security where new exploits are constantly being devised by attackers.

Some of the IT methods are not open or transparent. The details of the analysis are contained within computerized tools. Risk assessment approaches make explicit the basis on which decisions are made with regard to the implementation of cyber security measures.

Ideally, IT, control system and value chain cyber security should be addressed by the same methods, and possibly even within the same study. Even better is the ability to incorporate physical security into the analysis.

Three security vulnerability analysis (SVA) methods have previously been described by the author and applied to computer control systems. SVA is a form of risk assessment. The methods employ structured brainstorming, a technique that has a long history of success in the safety field. The methods can be used to study cyber security for any type of computer system including the manufacturing value chain and IT systems. This paper describes such applications.

Studies using the methods described can be performed as adjuncts to existing SVAs

that have focused on physical security, as part of future SVAs, or as stand-alone cyber SVAs (CSVA). The methods can also be used to consider all types of security issues in a single analysis including physical, personnel, information and cyber security, or any of these areas may be studied individually.

Introduction

IT cybersecurity is defined as the protection of the confidentiality, integrity and availability of information stored on computer systems. Typically, these are business systems used for management of finances, manufacturing, laboratory services, resource planning, communications, utilities, access control and other security functions, etc. Manufacturing and control system cyber security broadens this definition to include the protection of manufacturing and process control computer systems, and their support systems, from threats of cyber or physical attack by adversaries who wish to disable or manipulate them.

The manufacturing value chain includes those activities encompassed by distribution and transportation including warehousing, packaging and repackaging, and shipment (rail, road, marine, pipeline). It also includes relationships with suppliers, customers, service providers and toll producers.
Therefore, in order to address all types of computer systems, cyber security can be defined as the protection of computer systems of any type, and their support systems, from threats of cyber or physical attack by adversaries who wish to disable or manipulate them to cause harm, and access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information. Note that a cyber attack may be mounted to obtain sensitive information to plan a future physical or cyber attack.

This paper demonstrates how cyber SVAs can be performed for different types of computer systems using asset-based, scenario-based and sneak-path SVA methods that have been developed previously to address both cyber and physical attacks (1,2,3,4).

All the methods described are performance-based. They do not require the use of any specific risk remediation measures or countermeasures. Some companies may wish to prioritize systems for analysis. Methods have been described for screening cyber systems and physical systems(6).

The methods offer flexibility in their application and can be expanded or abbreviated to meet the needs of different users. They are structured around a classical risk analysis framework and are designed so they can easily be updated and modified to benefit from future technical developments and refinements.

The methods can address vulnerabilities at varying levels of detail to accommodate the needs of different companies. Some companies may have complex systems that require detailed analysis while others may have relatively simple systems that can be analyzed straightforwardly.

SVA Methods

SVA methods share a number of points in common. They all address:

Assets to be protected. They are entities that have value to someone and include cyber and physical assets. Cyber assets include software, hardware, data and peopleware (the people who interact with them). Physical assets include manufacturing equipment, materials and facilities, and support systems for cyber and physical facilities. (See checklists of assets in Attachment 4.) Assets have value both to the company and to attackers, but for different reasons. They are of value to a company because they are needed to conduct operations. They are of value to an attacker when they can be used to inflict harm, either to their owners or others.

Attackers or adversaries. These may be may be individuals, groups or organizations that conduct activities deliberately, or have the intention and capability to conduct activities, to attack assets. They may be insiders such as disgruntled employees, or outsiders such as hackers, or the two may operate in collusion. (See checklists of attackers in Attachment 4.) An attack is hostile action taken by an adversary to obtain access to an asset and use it to cause harm. Typical attack objectives will be to deny the use of the asset, damage or destroy it, or divert it to some other purpose. Objectives may include the release of hazardous materials; the theft of chemicals for later use as weapons or other misuse; the contamination of chemicals or tampering with a product that may later harm people; and damage or disruption to a plant or process. Attacks are specific deliberate actions taken by an adversary with the intent to cause harm.

Threats. They represent the possibility of hostile action towards an asset such as damage, destruction, theft, diversion or manipulation. (See checklists of threats in Attachment 4.) An analysis is usually performed to consider the likelihood that particular assets will be attacked by specific attackers. The motivation, intent, capabilities and resources of attackers are considered together with factors that influence the likelihood that a system will be targeted. The analysis is used to screen higher risk threats for consideration in vulnerability analysis.

Vulnerabilities. These are flaws or weaknesses that can be exploited by an adversary to successfully attack an asset.(See checklist of vulnerabilities in Attachment 4.)

Countermeasures (also called controls). These are secureguards that address the security of systems and safeguards that help ensure systems remain safe from attack. (See checklists of countermeasures in Attachment 4.) SVA considers the presence of existing countermeasures in assessing risk levels.

Consequences. These are the impacts of attacks. They may affect people, property, the environment, processes, products, companies, local communities, society, the nation, etc. SVA identifies these impacts. (See attachments 4 and 5 for examples.)

Risk estimates. SVA usually identifies the likelihood and severity of attacks to estimate the risk of attacks, often in the form of a risk ranking. (See discussion and example risk ranking scheme in Attachment 5.)

Recommendations. Actions that can be taken to reduce the risk to tolerable or acceptable levels are identified. (See discussion of study follow-up in Attachment 3.)

The asset-based, scenario-based and sneak-path SVA methods differ only in how they address these items:

Asset-Based SVA

This method considers how cyber assets can be exploited by attackers to cause harm. Threats are paired with assets to define *threat events* and the method considers vulnerabilities to attack, existing countermeasures to protect systems and the need for new or improved countermeasures. The analysis is not as detailed as in scenario-based methods but it provides results quickly and identifies overall protective measures.

Scenario-Based SVA

This method identifies ways specific threats can be realized (called *threat scenarios*) in a similar way to identifying hazard scenarios in a Process Hazard Analysis (PHA). A threat scenario is a specific sequence of events that has an undesirable consequence resulting from the realization of a threat. It is the security equivalent of a hazard scenario. Once vulnerabilities have been determined, recommendations may be made for consideration by management based on the nature of the threat, vulnerabilities, possible consequences and existing secureguards and safeguards.

Sneak-Path SVA

Sneak path analysis is used to identify the paths or ways (vulnerabilities) in which threat sources (attackers) may access cyber assets to cause harm. Existing barriers (countermeasures) to protect cyber systems, the events that may occur, and the need for new or improved countermeasures are addressed. The method provides a conceptually simple framework for conducting security vulnerability analysis that offers elements of both asset-based and scenario-based methods.

Applying SVA To Different Types of Computer Systems

In this section similarities and differences in applying SVA to different types of computer systems are discussed.

Types of Computer Systems

Business computer systems include:

- Enterprise Resource Planning (ERP)
- Global Enterprise Management System (GEMS)
- Supply Chain Management (SCM)
- Customer Relationship Management (CRM)
- Communications systems.
- WAN
- LAN

Manufacturing and Control computer systems include:

- Manufacturing execution system (MES)
- Laboratory Information Management System (LIMS)
- Manufacturing control system (MCS)
- Computerized Maintenance Management System (CMMS)
- Safety systems
- Utility systems

Computer systems used in the value chain include those identified in Table 1. There is overlap between the computer systems used for business management, manufacturing control and the value chain. Connectivity between these systems suggests that addressing cyber security comprehensively is the preferred approach.

Locations of Computer Systems

Business computer systems are typically located at corporate headquarters, individual plant sites, or other locations such as supplier, customer, service provider, or contractor facilities. Computer control systems are usually located at an individual plant site or at a remote location. Value chain computer systems may be at any of these locations or they may be mobile, e.g. on trucks.

Assets

IT cyber security is concerned with the confidentiality, integrity and availability of information and data assets. Control system and value chain cyber security extend these assets to include equipment and materials that could be manipulated by access to control system and value chain computer systems.

Attackers

In principle, adversaries may be the same for all types of computer systems. However, certain adversaries may be more likely to target a particular computer system. For example, terrorists may target control systems if they believe manipulation could result in plant shutdown or a release of hazardous material. Adversaries intent on stealing chemicals may target the value chain and competitors may be more interested in IT systems.

Threats

Principal threats are likely to be theft, damage, destruction or access to information for business systems, manipulation for control systems, and diversion of materials for the value chain.

Vulnerabilities

In principle, vulnerabilities may be the same for all types of computer systems. However, some may be more significant or more likely for particular types of systems. For example, a dial-up modem in a control system may represent a greater vulnerability than one in a business system. Lack of encryption may be more significant for value chain activities and shoulder surfing may be more significant for business systems than other systems.

Countermeasures

In principle, current cyber countermeasures are similar for all types of computer systems, although this may change as technology advances. Some countermeasures are more feasible for particular systems, e.g. password protection for business and value chain systems. Others are more appropriate for particular systems owing to the different types of attack they are likely to experience. For example, encryption is likely to be more important for value chain systems than control systems.

Consequences

The impacts of attacks depend on the type of attack. These will likely vary for different systems. Thus attacks on manufacturing business systems are likely to impact primarily the company. Attacks on control systems could impact the public if they are manipulated to cause hazardous material releases as could attacks on the value chain if hazardous materials are diverted. Control system attacks resulting in process shutdown may be more likely and impacts on both the company and the public may result.

Risk Estimates

The process of risk estimation is similar for all types of systems. Risk ranking schemes may be tailored for each type of system but it is preferable to use a single system to allow threats to be compared for the different systems. In order to do so, a risk ranking scheme is needed that provides sufficient discrimination of likelihoods, and especially consequences, so that risks for one type of system are not forced into a single category. Usually, this means that at least four or five levels of severity and likelihood should be used. Each level should be defined carefully.

Recommendations

The process of developing recommendations is the same for all systems. Decisions on the need for new or improved countermeasures are based on the estimated risk level, existing countermeasures, the magnitude and type of consequences, and the type of threat.

Ways to Cause Harm

There are both similarities and differences in how harm can be caused to the different types of computer systems that are addressed in SVA:

Business Systems

C Theft of sensitive information.
C Damage or destruction to sensitive information.
C Blocking access to information.
C Denial of service.
C Fraudulent acts.
C Privacy violation.
C Physical attacks.
C Natural, man-made, and environmental threats.

Control Systems

C Disabling systems.
C Shutting down systems.
C Interfering with production
C Stealing, damaging or blocking access to information.
C Altering set points.
C Disabling alarms.
C Unauthorized operation of equipment.
C Contaminating or poisoning products.
C Causing releases of materials.
C Causing runway reactions.
C Physical attacks.
C Natural, man-made, and environmental threats.

Value Chain

C Disrupting the flow of materials.
C Delaying shipments.
C Delaying the provision of services.
C Substituting materials.
C Contamination of materials.
C Locating shipments to hijack or attack.
C Diverting shipments to unauthorized destinations.
C Re-routing shipments through sensitive areas to be attacked.
C Causing transportation accidents.
C Causing the release of materials during storage or transportation.
C Stealing, damaging or blocking access to information.
C Physical attacks.
C Natural, man-made, and environmental threats.

The credibility of these and other ways of attack must be considered in SVA.

Key Issues for Different Types of Computer Systems

Some issues differentiate the different types of systems and should be kept in mind when conducting SVAs. They include:

Business Systems

C Large numbers of people using them.
C Need for massive connectivity.

Control Systems

C Threat of process manipulation.
C Potential for high severity consequences.

Value Chain Systems

C Use of mobile systems.
C Frequent use of wireless and satellite transmission.
C Some assets are mobile and there may be a greater threat of diversion.
C Multiple system access points that may be less secure, e.g. consoles on trucks (2-way), and web points.

Examples of the Application of SVA Methods

In order to perform a CSVA, a knowledge of cyber threats and vulnerabilities is needed. Detailed guidance on using the methods is provided in other papers[1,2,3]. Attachments 1 through 5 provide some additional guidance and checklists to assist in the analysis.

Examples have been provided previously of the application of the asset-based, scenario-based and sneak-path SVA methods to control systems[1,2,3]. Figures 1 - 3 provide examples of the applications of these methods to IT systems and Figures 4 - 6 to value chain systems.

The asset-based SVA worksheet in Figure 1 displays threat sources and their intents in separate columns. The entries could be combined into a single column, although separate columns are desirable when threat sources may have more than one intent. This particular example worksheet does not display vulnerabilities or safeguards. Typically, in the interest of a speedy analysis they are considered when recommendations are developed and are not documented in asset-based methods. However, there is no reason that vulnerability and countermeasures columns cannot be added to the worksheet to provide for their documentation. This can be contrasted with typical scenario-based SVA where these columns are usually included (see Figure 2).

In the scenario-based example provided (see Figure 2), consequences are displayed before countermeasures in the worksheet. This is normally done when worst-case consequences are assumed (i.e. without the benefit of safeguards). It is also possible to place the consequences column after the countermeasures column since that follows the logical progression of the threat scenario. For example, in the sneak-path SVA example provided the events (akin to consequences) column appears after the barriers (countermeasures) column (see Figure 3).

Figure 4 shows the application of asset-based analysis to the value chain. It demonstrates how both deliberate acts and inadvertent data entry into a computer routing system for road tankers can be treated in the same analysis. (IT cyber security usually addresses accidental events together with deliberate ones.) The example also shows how physical security and natural events can be addressed at the same time as cyber security, if desired. Figures 5 and 6 show the application of scenario-based analysis and sneak-path analysis to the value chain, respectively.

The level of detail in asset-based analysis can be varied. For example, in Figure 1 each of the assets could be broken down further, e.g. individual data bases could be listed. The level of detail is usually greater in scenario-based SVA than in asset-based. However, in the examples provided here the level of detail has been kept the same to facilitate comparison of the methods.

Conclusions

The asset-based, scenario-based and sneak-path SVA methods can be used to address cyber attacks on any type of computer system. They can also be used to address physical security for facilities.

The asset-based method provides the advantage of quickly identifying the overall protective measures needed. The scenario-based approach requires more time and effort but can provide more detailed recommendations for protective actions. The two methods are structured so that it is possible to conduct the simpler, asset-based approach first and, if needed, transition smoothly into a scenario-based analysis, either for the entire facility or parts of it that would benefit in the opinion of the analysts.

Changes in manufacturing plants can occur frequently and threats may change even more rapidly. SVAs should be updated whenever any significant change occurs in the facility, the threats it faces, or other aspects that may affect the risk. SVAs should also be revalidated on a regular schedule to ensure they reflect the current facility configuration, potential targets and the present threats.

Endnote

Additional checklists and templates for the performance of SVAs are available from Primatech. The templates used to illustrate the technique described herein were generated using Primatech's software products PHAWorks® and SVAWorks®. Other software products or paper worksheets can also be used.

References

1. P. Baybutt, "Cyber Security Vulnerability Analysis: An Asset-Based Approach" Process Safety Progress, p. 220, December 2003, Vol. 22. No. 4.

2. P. Baybutt, "Cyber Security – Are Your Facility Computer Systems Safe From Attack?", Hydrocarbon Processing , p. 49, March 2004, Vol. 83, No. 3.

3. P. Baybutt, Sneak Path Security Analysis (SPSA) for Industrial Cyber Security, to be published.

4. P. Baybutt, "Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis", Process Safety Progress, p. 269, December, 2002.

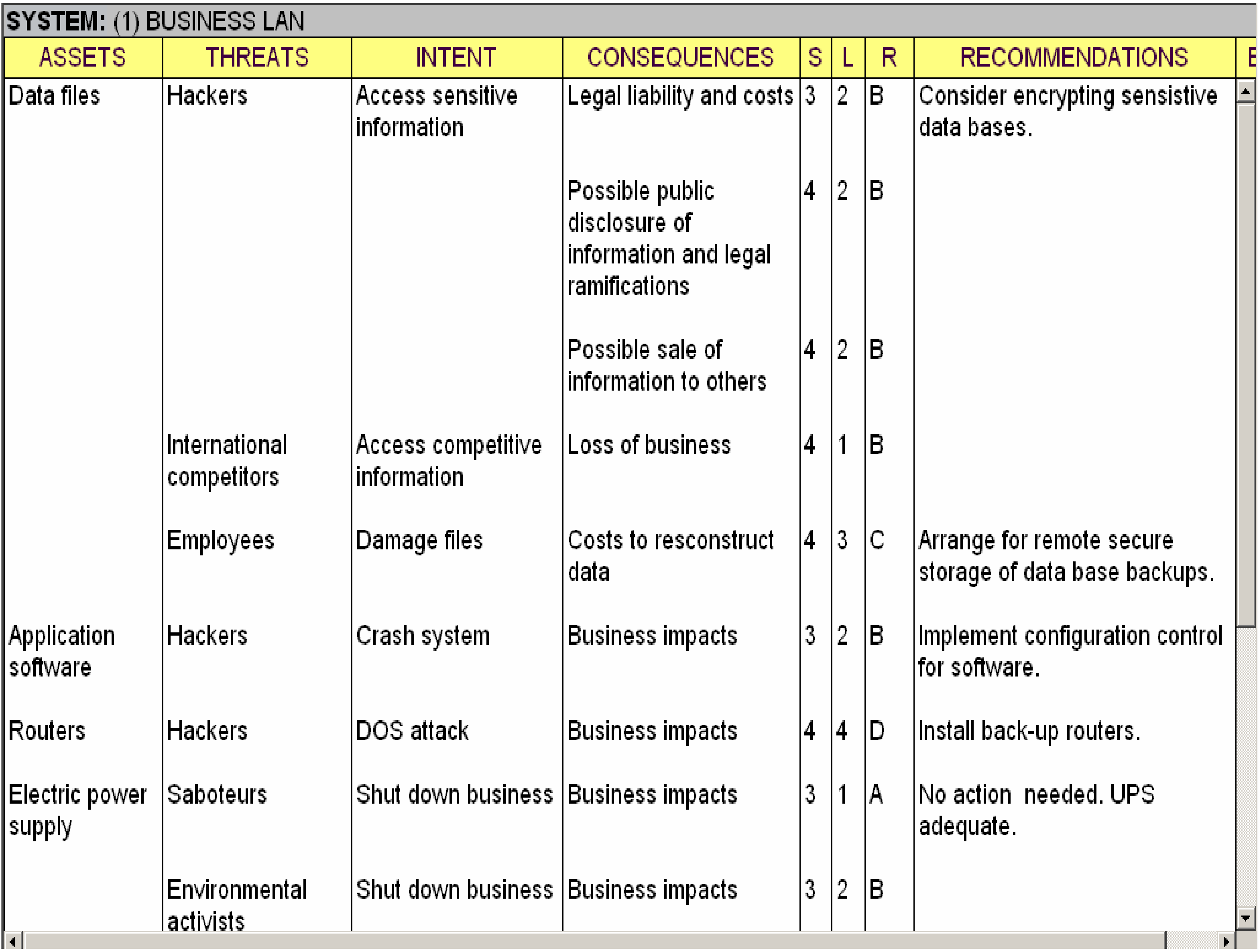
5. P. Baybutt, "Security Risk Analysis: Protecting Process Plants From Terrorism And Other Criminal Acts", to be published.

6. P. Baybutt, "Screening Facilities For Cyber Security Risk Analysis", to be published.

Table 1. Examples of Computer Systems Used In The Value Chain.

Value Chain Activity	Computer systems
Warehousing	Inventory management, environmental management systems, B2B system.
Packaging and repackaging	Control and conveyor systems, telemetry.
Shipment (rail, road, marine, pipeline)	Scheduling, routing, tracking, monitoring.
Suppliers	Supply Chain Management, Global Enterprise Management System, telephony systems.
Customers	Customer Relationship Management, Global Enterprise Management System.
Service providers	Trade exchange.
Toll producers	Customer Relationship Management, Global Enterprise Management System, process control.
Manufacturing	Customer Relationship Management, Global Enterprise Management System, Process Control Networks, B2B system, telephony systems, maintenance systems, LIMS, WAN, LAN, utility and safety management systems.

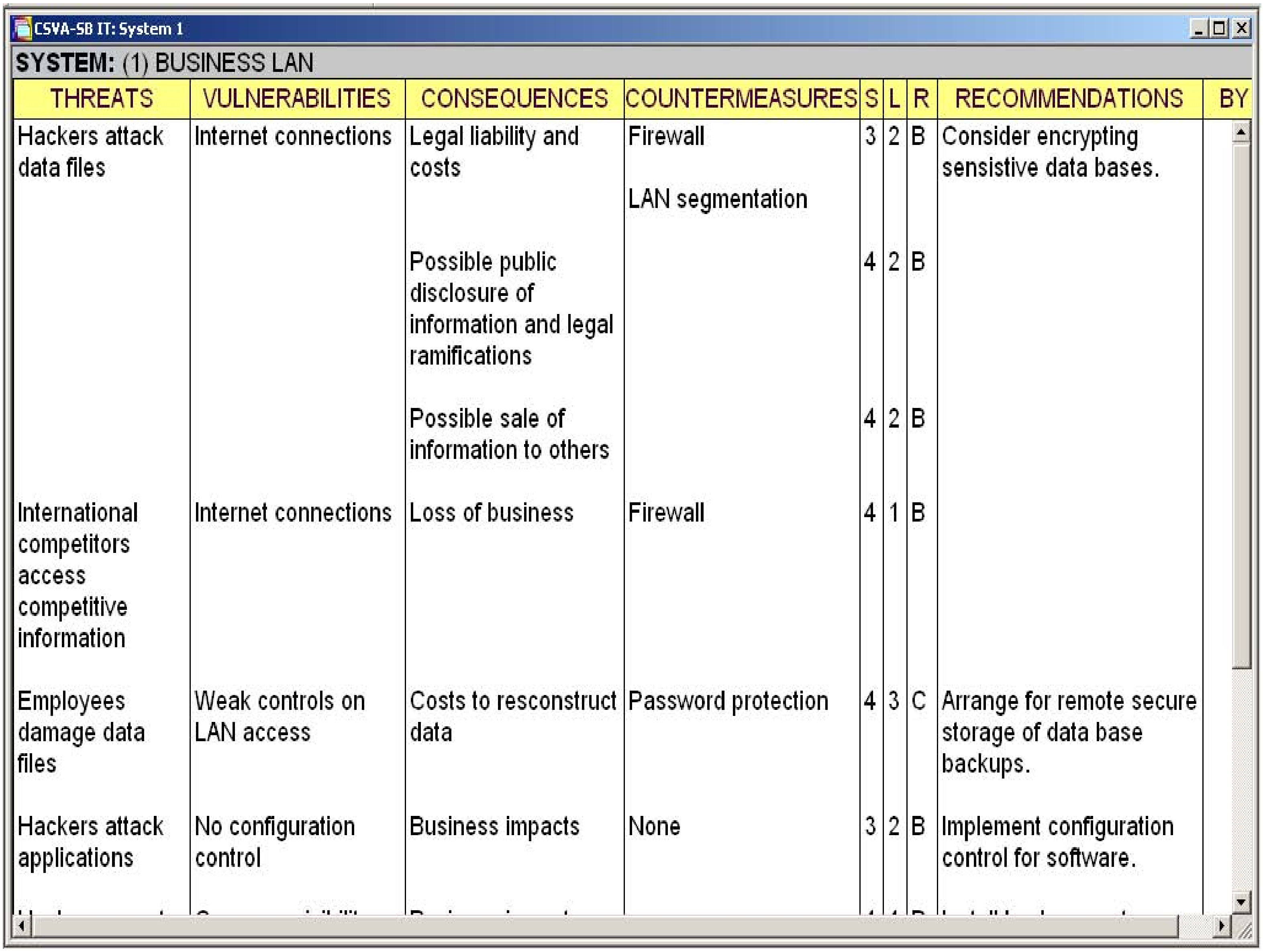
Figure 1. Asset-Based SVA for IT System.



SYSTEM: (1) BUSINESS LAN

ASSETS	THREATS	INTENT	CONSEQUENCES	S	L	R	RECOMMENDATIONS	E
Data files	Hackers	Access sensitive information	Legal liability and costs	3	2	B	Consider encrypting sensistive data bases.	
			Possible public disclosure of information and legal ramifications	4	2	B		
			Possible sale of information to others	4	2	B		
	International competitors	Access competitive information	Loss of business	4	1	B		
	Employees	Damage files	Costs to resconstruct data	4	3	C	Arrange for remote secure storage of data base backups.	
Application software	Hackers	Crash system	Business impacts	3	2	B	Implement configuration control for software.	
Routers	Hackers	DOS attack	Business impacts	4	4	D	Install back-up routers.	
Electric power supply	Saboteurs	Shut down business	Business impacts	3	1	A	No action needed. UPS adequate.	
	Environmental activists	Shut down business	Business impacts	3	2	B		

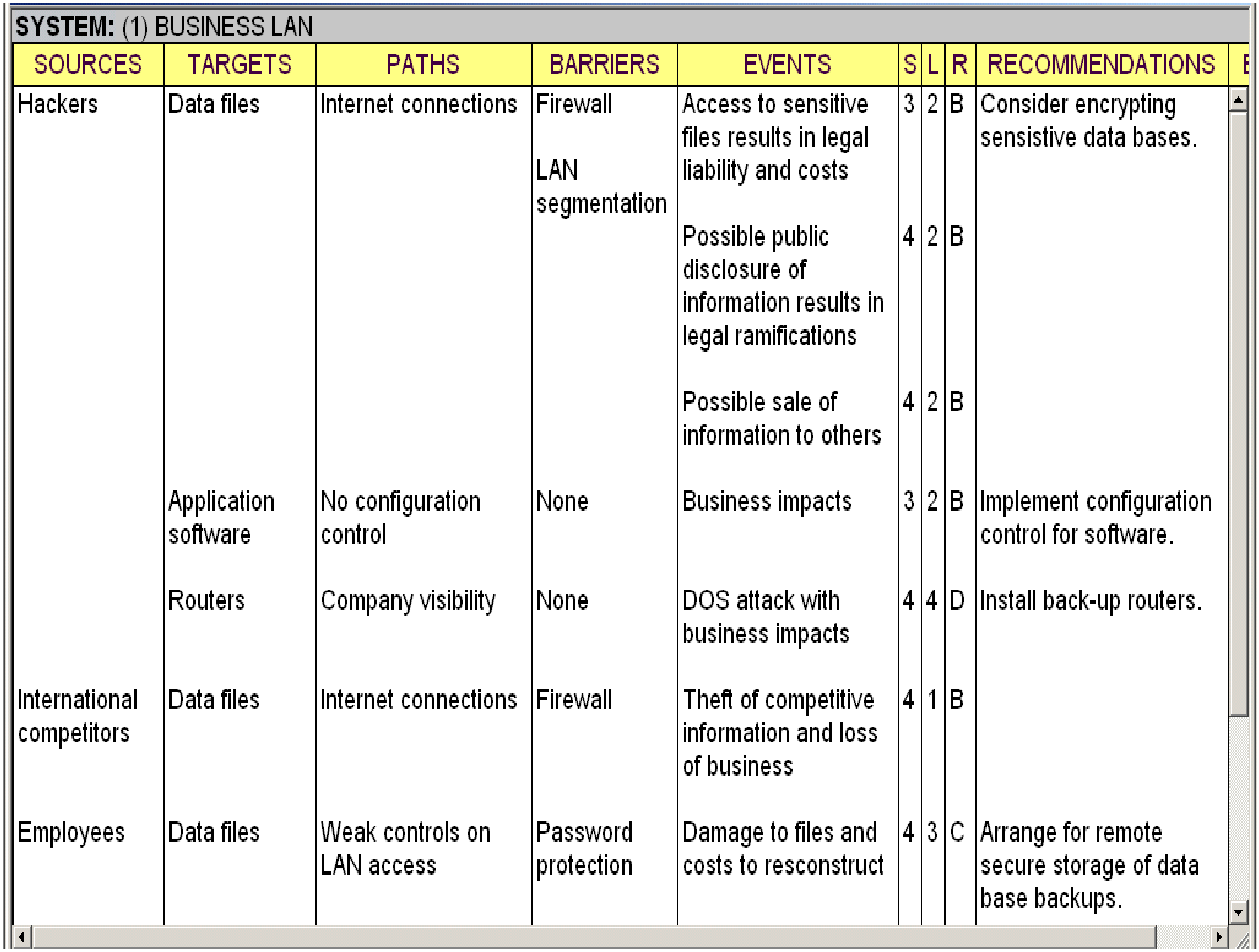
Figure 2. Scenario-Based SVA for IT System.



SYSTEM: (1) BUSINESS LAN

THREATS	VULNERABILITIES	CONSEQUENCES	COUNTERMEASURES	S	L	R	RECOMMENDATIONS	BY
Hackers attack data files	Internet connections	Legal liability and costs	Firewall LAN segmentation	3	2	B	Consider encrypting sensistive data bases.	
		Possible public disclosure of information and legal ramifications		4	2	B		
		Possible sale of information to others		4	2	B		
International competitors access competitive information	Internet connections	Loss of business	Firewall	4	1	B		
Employees damage data files	Weak controls on LAN access	Costs to resconstruct data	Password protection	4	3	C	Arrange for remote secure storage of data base backups.	
Hackers attack applications	No configuration control	Business impacts	None	3	2	B	Implement configuration control for software.	

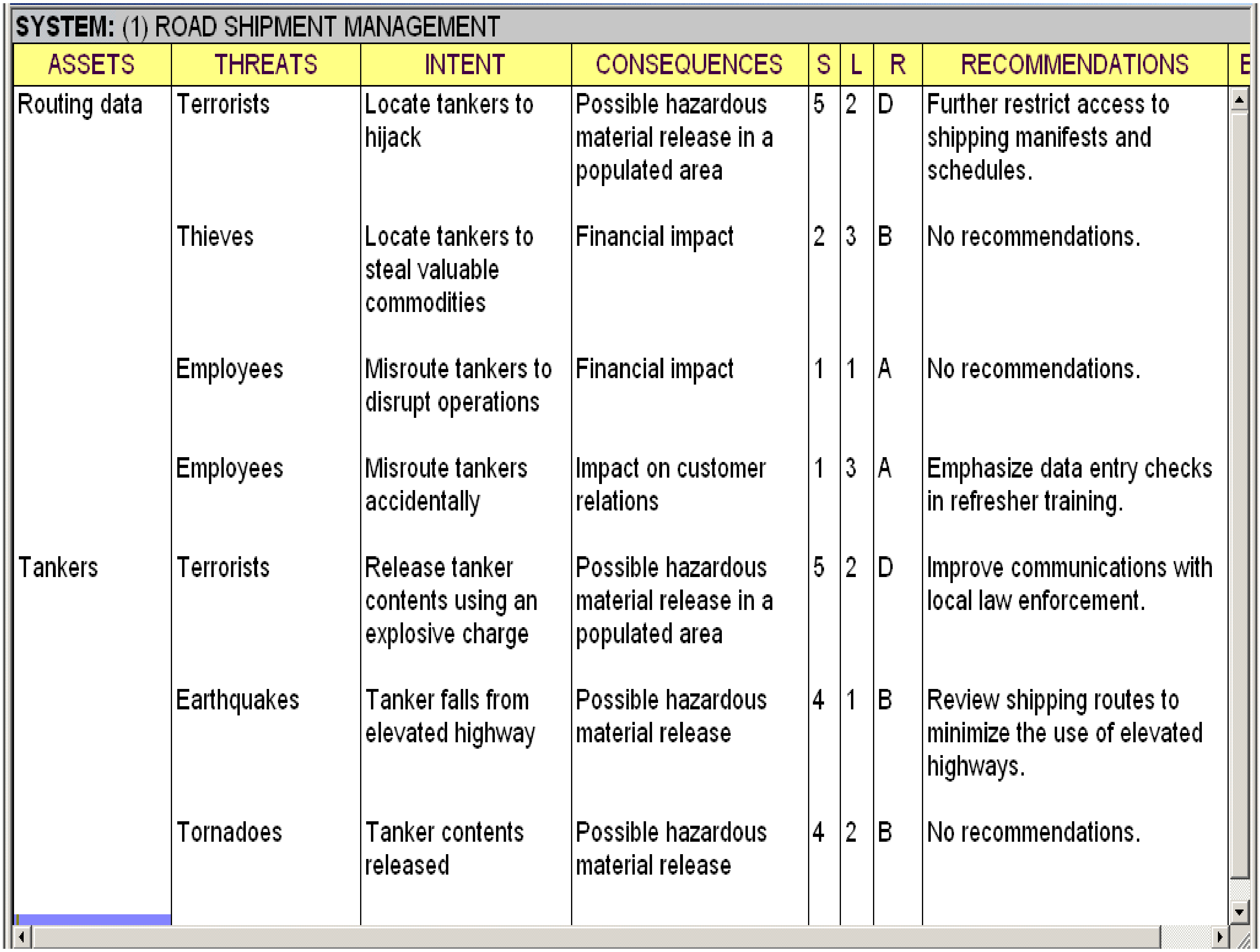
Figure 3. Sneak-Path SVA for IT System.



SYSTEM: (1) BUSINESS LAN

SOURCES	TARGETS	PATHS	BARRIERS	EVENTS	S	L	R	RECOMMENDATIONS	E
Hackers	Data files	Internet connections	Firewall LAN segmentation	Access to sensitive files results in legal liability and costs	3	2	B	Consider encrypting sensistive data bases.	
				Possible public disclosure of information results in legal ramifications	4	2	B		
				Possible sale of information to others	4	2	B		
	Application software	No configuration control	None	Business impacts	3	2	B	Implement configuration control for software.	
	Routers	Company visibility	None	DOS attack with business impacts	4	4	D	Install back-up routers.	
International competitors	Data files	Internet connections	Firewall	Theft of competitive information and loss of business	4	1	B		
Employees	Data files	Weak controls on LAN access	Password protection	Damage to files and costs to resconstruct	4	3	C	Arrange for remote secure storage of data base backups.	

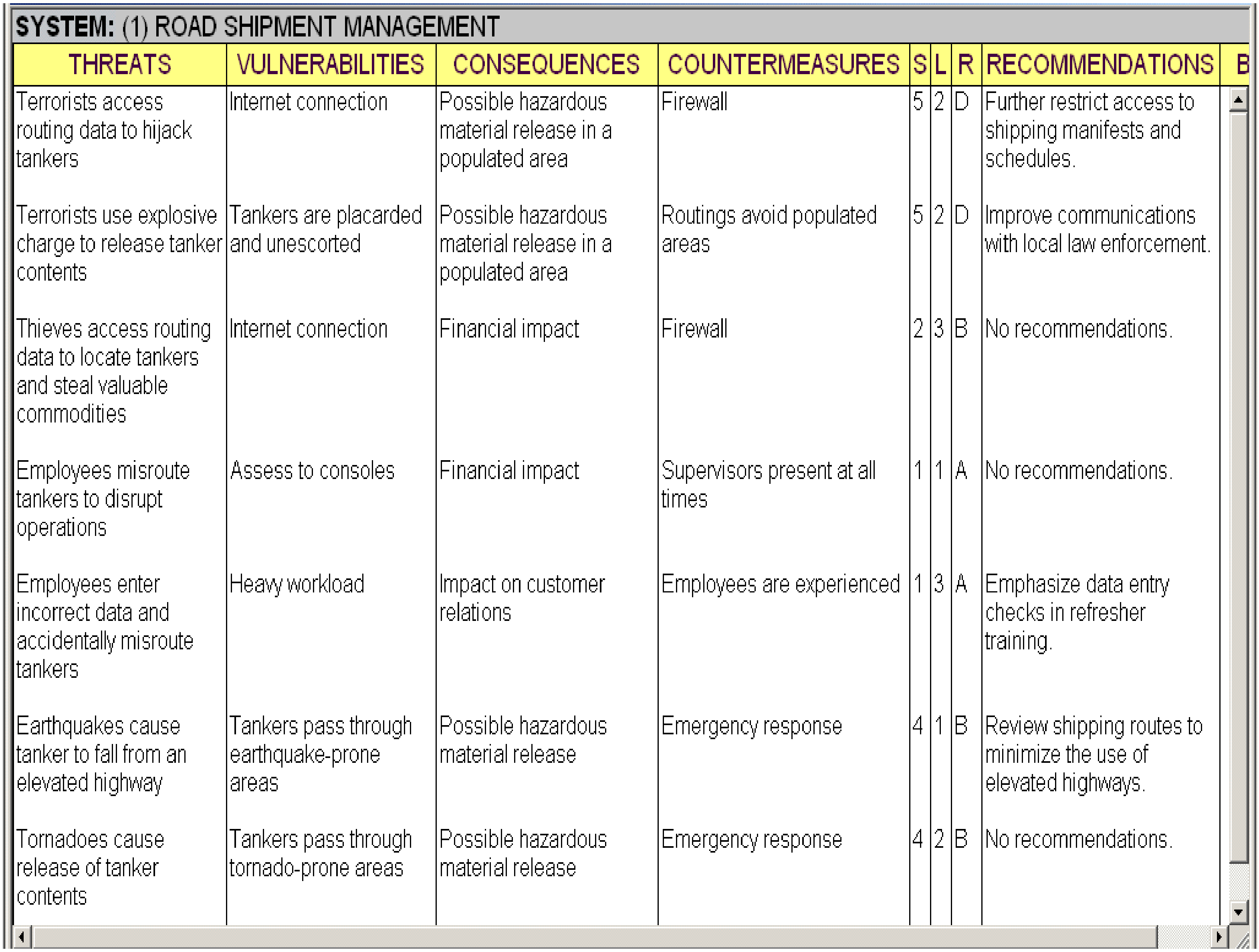
Figure 4. Asset-Based SVA for Value Chain System.



SYSTEM: (1) ROAD SHIPMENT MANAGEMENT

ASSETS	THREATS	INTENT	CONSEQUENCES	S	L	R	RECOMMENDATIONS	E
Routing data	Terrorists	Locate tankers to hijack	Possible hazardous material release in a populated area	5	2	D	Further restrict access to shipping manifests and schedules.	
	Thieves	Locate tankers to steal valuable commodities	Financial impact	2	3	B	No recommendations.	
	Employees	Misroute tankers to disrupt operations	Financial impact	1	1	A	No recommendations.	
	Employees	Misroute tankers accidentally	Impact on customer relations	1	3	A	Emphasize data entry checks in refresher training.	
Tankers	Terrorists	Release tanker contents using an explosive charge	Possible hazardous material release in a populated area	5	2	D	Improve communications with local law enforcement.	
	Earthquakes	Tanker falls from elevated highway	Possible hazardous material release	4	1	B	Review shipping routes to minimize the use of elevated highways.	
	Tornadoes	Tanker contents released	Possible hazardous material release	4	2	B	No recommendations.	

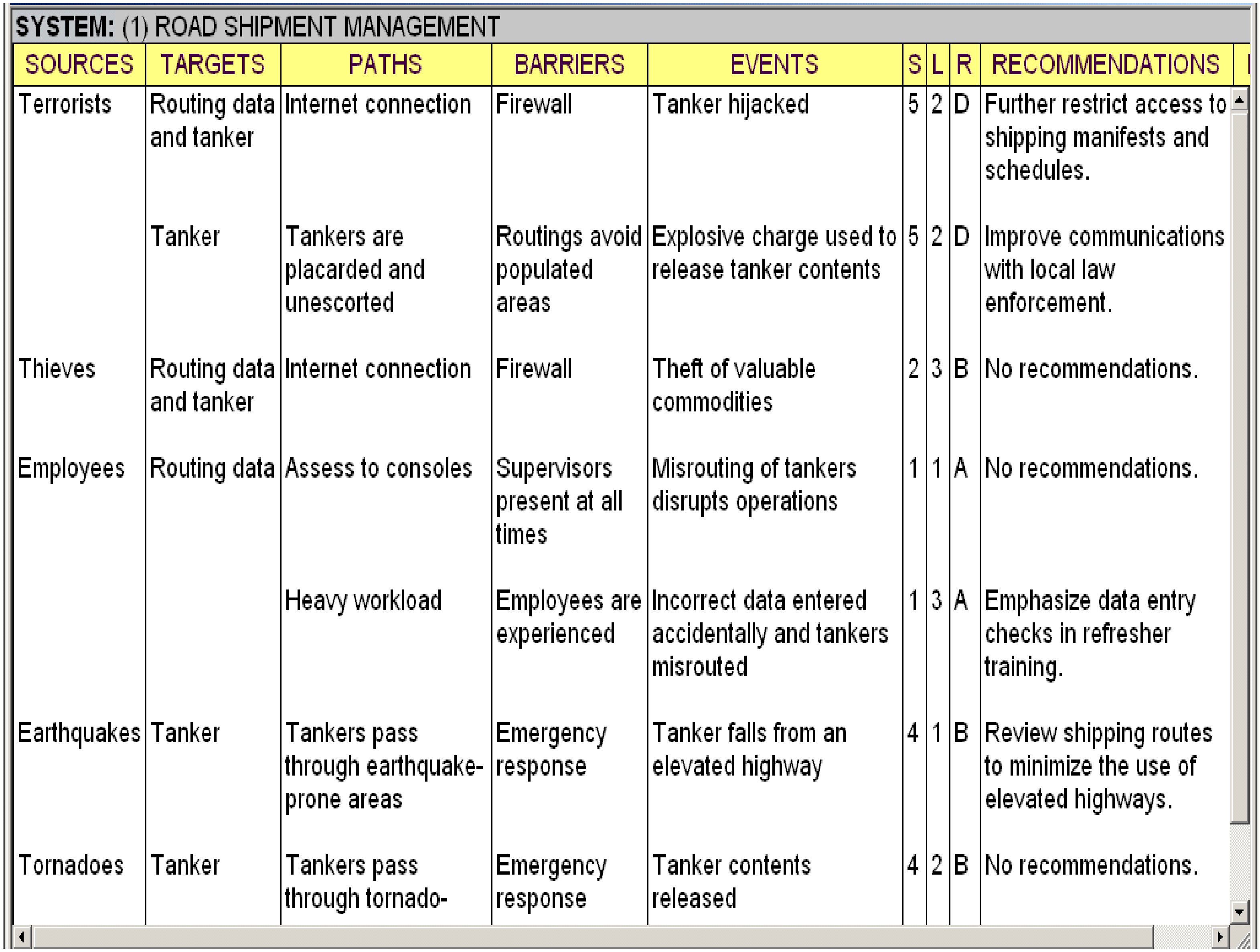
Figure 5. Scenario-Based SVA for Value Chain System.



SYSTEM: (1) ROAD SHIPMENT MANAGEMENT

THREATS	VULNERABILITIES	CONSEQUENCES	COUNTERMEASURES	S	L	R	RECOMMENDATIONS	B
Terrorists access routing data to hijack tankers	Internet connection	Possible hazardous material release in a populated area	Firewall	5	2	D	Further restrict access to shipping manifests and schedules.	
Terrorists use explosive charge to release tanker contents	Tankers are placarded and unescorted	Possible hazardous material release in a populated area	Routings avoid populated areas	5	2	D	Improve communications with local law enforcement.	
Thieves access routing data to locate tankers and steal valuable commodities	Internet connection	Financial impact	Firewall	2	3	B	No recommendations.	
Employees misroute tankers to disrupt operations	Assess to consoles	Financial impact	Supervisors present at all times	1	1	A	No recommendations.	
Employees enter incorrect data and accidentally misroute tankers	Heavy workload	Impact on customer relations	Employees are experienced	1	3	A	Emphasize data entry checks in refresher training.	
Earthquakes cause tanker to fall from an elevated highway	Tankers pass through earthquake-prone areas	Possible hazardous material release	Emergency response	4	1	B	Review shipping routes to minimize the use of elevated highways.	
Tornadoes cause release of tanker contents	Tankers pass through tornado-prone areas	Possible hazardous material release	Emergency response	4	2	B	No recommendations.	

Figure 6. Sneak-Path SVA for Value Chain System.



SYSTEM: (1) ROAD SHIPMENT MANAGEMENT

SOURCES	TARGETS	PATHS	BARRIERS	EVENTS	S	L	R	RECOMMENDATIONS
Terrorists	Routing data and tanker	Internet connection	Firewall	Tanker hijacked	5	2	D	Further restrict access to shipping manifests and schedules.
	Tanker	Tankers are placarded and unescorted	Routings avoid populated areas	Explosive charge used to release tanker contents	5	2	D	Improve communications with local law enforcement.
Thieves	Routing data and tanker	Internet connection	Firewall	Theft of valuable commodities	2	3	B	No recommendations.
Employees	Routing data	Assess to consoles	Supervisors present at all times	Misrouting of tankers disrupts operations	1	1	A	No recommendations.
		Heavy workload	Employees are experienced	Incorrect data entered accidentally and tankers misrouted	1	3	A	Emphasize data entry checks in refresher training.
Earthquakes	Tanker	Tankers pass through earthquake-prone areas	Emergency response	Tanker falls from an elevated highway	4	1	B	Review shipping routes to minimize the use of elevated highways.
Tornadoes	Tanker	Tankers pass through tornado-	Emergency response	Tanker contents released	4	2	B	No recommendations.