THE INTERNATIONAL MARITIME TRANSPORT & LOGISTICS CONFERENCE
(MARLOG 4)
A SUSTAINABLE DEVELOPMENT PERSPECTIVE FOR MEGA PROJECTS
29- 31 MARCH 2015

MODELING RESILIENCE OF SECURITY SERVICES' SUPPLY CHAIN

WAEL FARGHALY

Chief Executive Officer, Knowledge Towers LLC, and
Visiting Lecturer, College of International Transport and Logistics,
Arab Academy for Science, Technology, and Maritime Transport
Nasr City, Cairo, Egypt,
w.farghaly@knowledgetowers.com

ABSTRACT: Ports, business facilities, shipping vessels, and housing compounds are all manageable through organizational management systems[1, 2, 3, 4]. Moreover, they all require protection against possible internal vulnerabilities and external threats[4, 5, 6, 7, 8]. Nonetheless, they need resources to respond to disruptions caused by crises or disasters. This protection appears in organizations' security services. When investigating organizational resilience, security systems prove to be essential components of organizations' resilience[1, 6, 9, 10]. They carry out specific roles and responsibilities in prevention, preparedness, mitigation, response, continuity, and recovery processes after a business disruption event[7, 11].What happens if the security service's supply chain experiences disruption? What is the supply chain of security services like? What factors affect the resilience of that service? Moreover, what are the potential disruption incidents that can take place? This paper proposes three supply chain models for the security services that are applicable to most of the organizations. In addition, it defines the resilience in the supply chain of security services and identifies two KPI's through which, organizations can measure the resilience security services' supply chain. Furthermore, this research proposes the use of reliability models to measure the identified KPI's.

Keywords: Security Services, Supply Chain, Resilience Modeling, KPI's, Reliability Models

INTRODUCTION

This introduction highlights the essential information to facilitate the understanding of the research topic. It includes a brief about the relation between security services and business continuity. It introduces a snapshot about the research methodology while more explanation appears in its designated section. In addition, it explains reliability modeling according to the scope of this research.

SECURITY SERVICES IN LIGHT OF BUSINESS CONTINUITY

Security services represent a necessary component in business-continuity-management systems[7, 11]. Security services support different business functions in the event of disruption.

Whether in-house or outsourced, those services may experience disruption; for example, a crisis takes place at a location, and the security team responsible for protection has been working for over 12 hours and some members of the replacement shift cannot reach the location because there is transportation disruption. The team that is already in place may not be able to continue around the clock. Therefore, it is necessary to find possible solutions to such a problem before that event takes place. This research explores similar problems and their solutions from the perspective of Supply Chain Resilience (SCR).

In order to produce the aforementioned solutions, in this context, problem identification must be made first. Thus, there must be a risk register for potential disruption to the security services supply chain[12]. Nonetheless, there must be a supply chain model to conduct the required disruption assessment over its different nodes. Therefore, the first step in this research is to establish the supply chain model. The second is risk assessment across that model. The next step is the planning phase during which, the necessary contingency plans are developed to respond to the disruption incidents.

When contingency plans are in place, there must be a measurement method to identify the level of performance. This measurement will require the establishment of viable KPI's. Finally, there comes the necessity to develop the model that allows the organization to measure those KPI's.

This research introduces reliability models as a tool to measure the security services supply chain resilience KPI's. Reliability models will quantify each KPI's in a value that ranges from 0 to 1. This will require the selection of measurement criteria and the substitution for each criterion with a numerical value that can be used in the measurement model. The conversion of the selection criteria to numerical values will be subject to binary data systems. Thus, if the criterion is available or performing, the criterion will be represented by the value 1. If the criterion is not available or not performing, the criterion will be given the value 0.

There are three possible models for reliability[13, 14]. The series model represents a system that the entirety of its components must function in order for the system to work properly. The parallel model requires that a redundant component or subsystem is available to execute the same task or process in case the primary component is not functional. The last model is the k-out-of-n model. This model requires only a certain number of components to function in order for the system to be working. Parallel and k-out-of-n models will produce better reliability results. However, they are not applicable to this research. In order to apply parallel or k-out-of-n models, the security system must be redesigned to provide for redundancy for all or part of the system.

Figure 1 displays the series and parallel models; where R_S is the system reliability; R_1 is the reliability of the first subsystem or component up to R_n, where n represents the number of all the subsystems or components. The equation for each model is below its corresponding model in figure 1[13, 14].

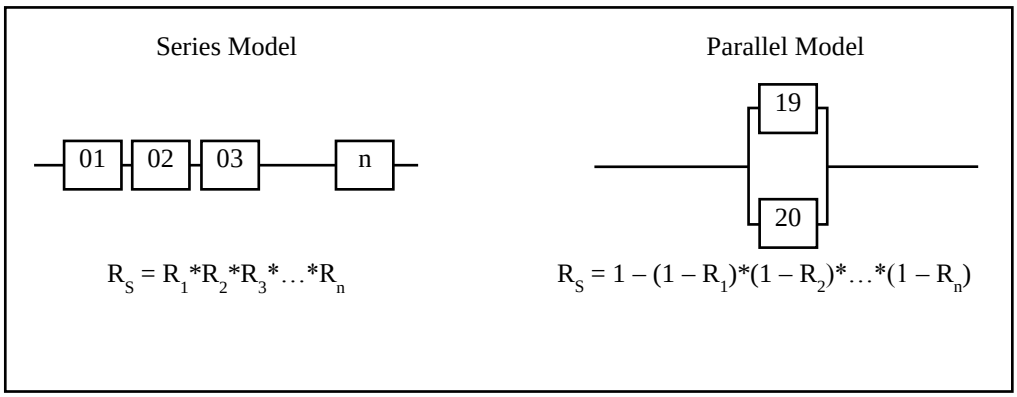

Figure (1) Series and Parallel Models

SECURITY SERVICES SUPPLY CHAIN MODELS

The supply chain consists of all the companies, firms, organizations and individuals that perform or produce goods and services that are necessary to the introduction of the final products (goods or services) from the point of origin to the point of delivery[2, 3, 4, 15, 16]. Therefore, security services supply chain will include all the activities and processes that make the service available to the customer. This includes human resources (HR) and procurement functions, capacity building firms, and security equipment suppliers and manufacturers, etc.

Identifying the stakeholders to the security services enables the formation of a comprehensive supply chain model[2, 3, 17]. The method of offering the services will vary according to the needs of the organization and the criticality of the service to the organization; for example, a classified government facility may require that all security elements are internal employees due to the confidentiality of the work carried out in that facility. In this situation, there will be no security service provider in the firm supply chain. However, the organization procurement system will purchase the necessary equipment and the HR will conduct the necessary recruitment of security personnel. Therefore, the organization will need to build relations with equipment suppliers and the HR will need to build relations with the recruitment agencies and the training firms that will provide the necessary training for the newly hired security personnel. All of these activities and more will appear as essential components in the security services supply chain.

SECURITY SERVICES INSIDE THE ORGANIZATION

Security services appear in different types of facilities as an in-house, outsourced, or a mixed team of both in-house and outsourced personnel and equipment. Mostly, the security management will be of the firm main staff and the guards will be outsourced. Security personnel are not the only components of a security system. Security services require certain

types of equipment to execute the required processes[14]. This provides for three possible supply chain models: 1) fully in-house system, 2) fully outsourced system, and 3) mixed system.

SECURITY SERVICES SUPPLY CHAIN STAGES

This research identifies five stages in the security services supply chain. Stage 1 includes all the suppliers of material to the manufacturers or security-training providers. Stage 2 includes the manufacturers, training-service providers, and may include the labor market for the security service provider where the selection of security personnel takes place. Stage 3 includes the distributors of equipment and may include the labor market. Stage 4 represents the organizational functions that perform the security services acquisition processes in favor of the organization such as procurement and human resources. The last stage, stage 5, is the internal customer of the organization's procurement and human resources, which is the facility, assets and employees on the premises.

This research provides the supply chain models as examples. However, the research does not include the study of SCR of all the models, nor does it study all the nodes and the possible disruption incident that may occur. A comprehensive study of the three models and the nodes in each one may require an empirical research applied to an organization. That study; however, will also lead to the study of only one model, the one that applies to the organization.

THE FULLY IN-HOUSE MODEL

In the fully in-house model (figure 2), the entire security system is a main component of the organization's structure. All the system personnel are employed as main staff in the organization and all the security equipment is logged in the organization's fixed assets. Firms adopt this model when the security function is critical to business. For example, an important governmental organization. In this model the security service provider does not appear anywhere in the supply chain.

In order to fit the figures, the abbreviation "Equip. Manu." Stands for equipment manufacturers, "Equip. Supplier" stands for equipment suppliers, and "Procure." Stands for the procurement function.

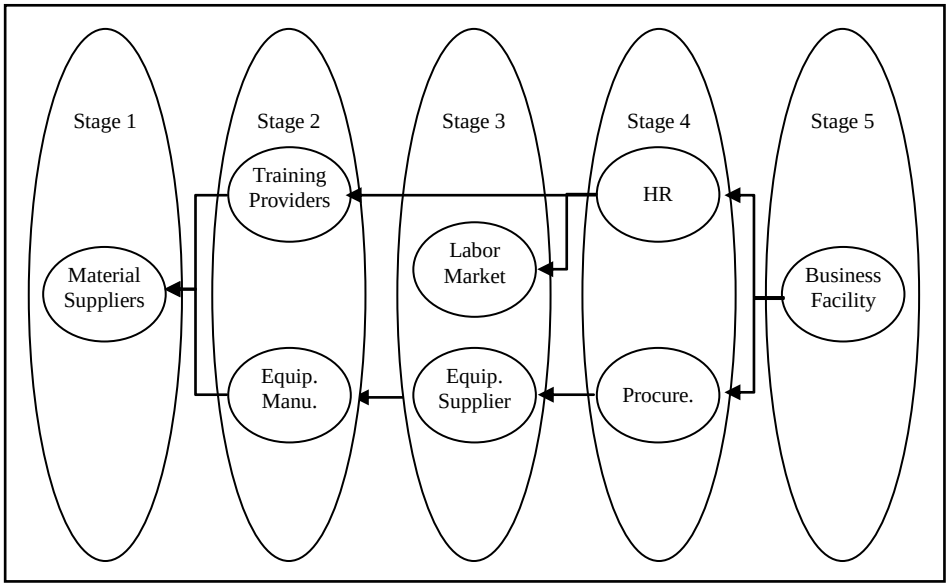

Figure (2) Supply chain model for fully in-house security systems

THE OUTSOURCED MODEL

Firms tend to adopt this model, (figure 3), when security is not a critical business function. Therefore, the organization chooses to outsource the entire system including the equipment. This may happen when the organization is in the inception phase, or when the organization is operating at a temporary location.

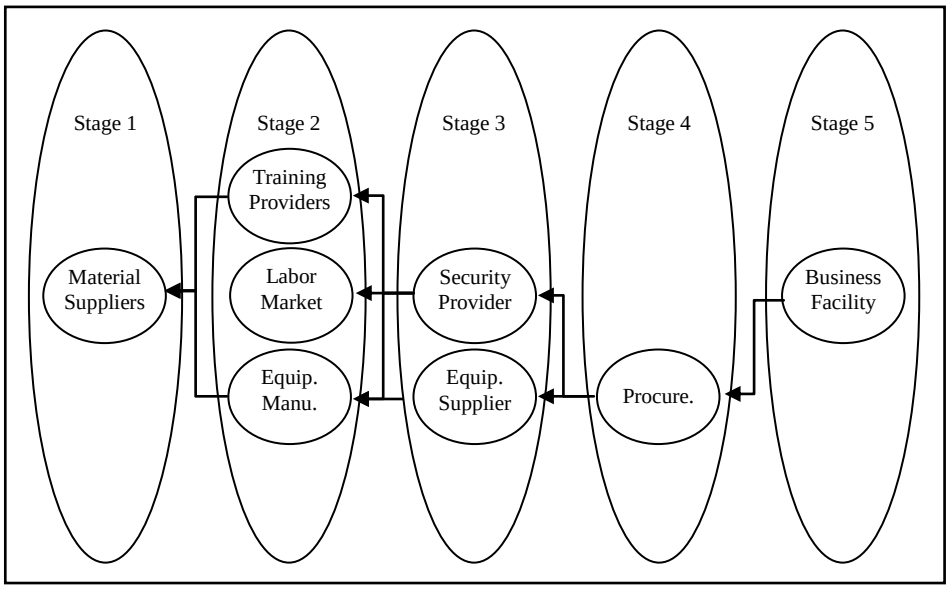

Figure (3) Supply chain model for outsourced security systems

THE MIXED MODEL

This is the most common model (figure 4). The organization will most probably hire the top management of the security team. The firm may purchase some or all the equipment needed for the system to perform the required security processes. The middle management and guards of the team will be outsourced.

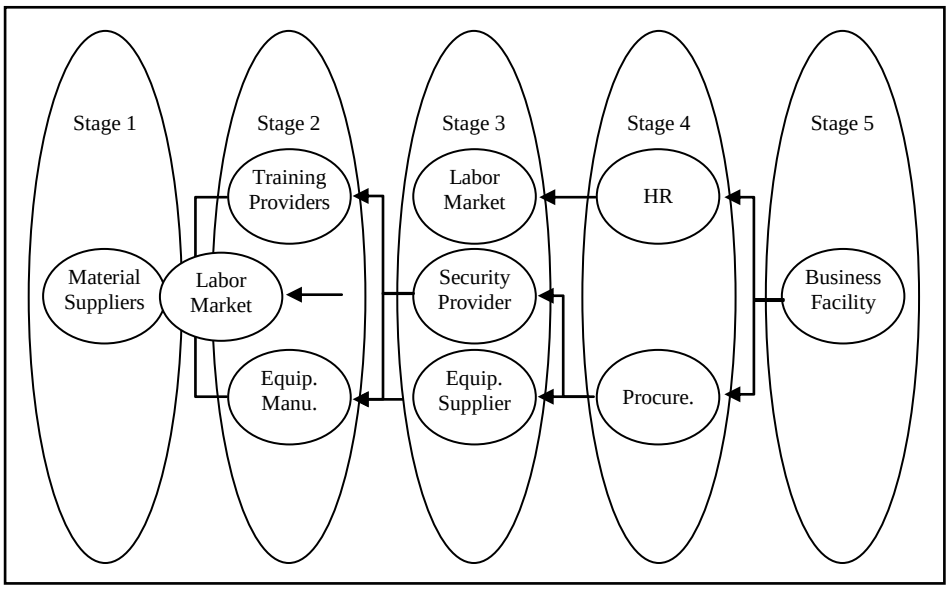

Figure (4) Supply chain model for mixed security systems

IDENTIFYING KPI'S OF SECURITY SERVICES SCR

Supply chain resilience is the ability of the supply chain to handle a disruption event without a significant impact on the ability to serve the customer[1, 3, 7, 18, 19]. In the context of security services supply chain, resilience will simply be the ability of the security services supply chain to deliver the services to the customer whether internal or external with the minimum possible impact on other business functions. Disruption here may not only be a crisis or a disaster, but it can also be a technical deficiency in the equipment necessary to perform the security system processes; for example, it can be the malfunction of the weapon-detection equipment, which may lead to the illegal entry of weapons to the facility.

Security services SCR KPI's depend on whether the security system will have the capacity to perform in the event of disruption[1, 3, 5, 7, 19]. Some of the items in the supply chain may be irrelevant to that capacity; for example, the supply of guards' uniform. An essential KPI may concern the security system capacity to perform certain security processes in the event of disruption with acceptable level of reliability.

Disruption in the security services supply chain may occur due to the lack of personnel, deficiency of necessary equipment, dispersed system processes, or a wrong course of action to follow when the disruption incident takes place. Therefore, an organization needs to identify

all the possible disruption incidents and devise suitable contingency plans to respond to those incidents and select the suitable risk management strategy. Thus, the firm must be ready to handle the disruption. In addition, the organization must be able to perform the contingency plans in a timely manner. To conclude, the organization must be ready with the plans and the capacity to execute them.

This research identifies two KPI's that will measure the supply chain resilience. Those two KPI's are preparedness and performance in the event of disruption. Preparedness includes risk identification, laying down the appropriate contingency plans, and the training of elements to carry out those contingency plans. Performance in the event of disruption will be measured using reliability models to assess the system capacity, including trained employees, to perform the contingency plans. The following two sections will detail the work needed on preparedness and performance.

PREPAREDNESS KPI

Preparedness is a major key in SCR[1, 6, 8, 10, 12, 18, 19, 20, 21, 22]. It simply shows that the organization has identified the potential risk, developed the necessary contingency plans, and built its capacity to manage the disruption incident. In the case of security services, this means that the organization has studied the potential risk for the security services supply chain, designed the plans to meet those risks, and trained the people who will carry out the work required by the contingency plans.

For example, one of the risks to the security system is the shortage in security personnel to carry out the needed work. Are there substitutes? Some of the organization's employees must be trained to carry out the security processes. In some countries including Egypt, Labor Law mandates that at least 25% of the employees are trained in Civil Protection. Organizations, driven by their benefits, may develop a policy that a certain percentage of its employees are trained to execute the security plans designed in the risk register to achieve the best possible security services resilience. Eventually, the resilience of the security system is a part of the overall organizational resilience.

The factors to be measured in the preparedness KPI are:

1. The availability of a security-service-resilience risk register that is up-to-date.
2. The viability of the contingency plans of identified risks.
3. The availability of trained non-security employees to execute the contingency plans.

THE RISK REGISTER

This research does not provide a comprehensive risk register through a certain supply chain model. This is due to the intensity of the work carried out in the research in addition to some limitations such as the lack of an organization where the research can be applied, and the funds needed to execute such a massive scale of work. However, the sample of identified risks in the given example are true and they happened before. Unfortunately, the research

cannot state the detailed incidents because it may be considered as an act of defamation for the involved organizations.

In developing a real-time risk register, the organization's representative may select the supply chain model that suits the organization, or chooses to adapt one of the models to the organizational structure. The following identified risks are selected based on the possibility to take place at any of the three proposed models. The given responses are not the only possible solutions and they cannot be carried out by all the organizations. Thus, response planning will depend on the organizations policies, funding capabilities, knowledge assets, etc.

A key element in the construction of the security-services-supply-chain risk register is that it should be revisited at least on quarterly basis. It is better for the organization if a security-consulting firm approves the risk register. In addition, the roles and responsibilities of all stakeholders must be clear and easy to understand. Table 1 includes a proposed risk register for the security services supply chain. In the table, SR stands for Security Risk.

Table 1. Example: Security Services Resilience Initiative Risk Register

Risk Identification		**Response Planning**		**Risk Monitoring and Control**	
RID	*Threat*	*Response Plan*	*Owner*	*Status*	*Notes*
SR1	Lack of enough security personnel to perform the required security processes due to security employees' strike. All facility entry doors need protection.	P1. Train 10% of company employees on security processes. P2. Close all the entry doors and stick to one entry point.	Head of Security and Head of Crisis Management	In progress	Training completes on April 12, 2015
SR2	CCTV system is down and there are no maintenance spare parts because the system is discontinued.	P1. Relocate the working cameras in the most critical areas. P2. Study the viability of installing a new system. P3. Issue a priority list of locations covered by CCTV.	Head of Security and Head of Procurement	Approved	New system procurement from the risk management budget if available.
SR3	The electronic gate for weapon detection at the facility entrance does not function.	P1. Use handheld scanners.		In progress	

The sample risk register indicates that disruption to the security system does not come only from the shortage in personnel. It indicates as well that disruption may occur due to equipment malfunction such as the closed circuit television (CCTV) system. CCTV systems play a great role as an incident prevention tool, which is costly if the organization tries to replace it by guards.

Some people may argue that the above solutions are common sense and they do not need a risk register. The answer simply lies in the following benefits:

1. The risk register grants the organization enough time to consider, develop and review the best contingency plans available.
2. It improves the security-service-supply-chain responsiveness since the lag time consumed by the attempts to find the solutions and the time to get the top management approval will be eliminated.
3. It ensures that all the nodes of the supply chain have been investigated for potential risks.

THE CONTINGENCY PLANS

The contingency plans viability needs to be investigated. Thus, the work needed in the contingency plan must be financially viable. For example, in case the CCTV system is down the organization will replace them with security guards equipped with walkie-talkies to report any illegal intervention. This is not viable because of the following:

1. The cost will be very high.
2. The camera does not take breaks while the guard may need a break, which will incur the hiring of extra replacement guards, which in turns will increase the costs to a higher level.
3. The guard will not be able to cover the same area the camera can because the camera is usually installed in a high place in the facility.
4. The camera enables the recording of events and retrieving those recordings later, while the guard cannot do the same.
5. The camera recording will be objective in the details of the incident but the guard may become subjective.

THE TRAINING OF THE NON-SECURITY EMPLOYEES

In the selection of the non-security employees, there are some criteria to be addressed. These criteria can be modified according to the organization's structure. Therefore, the evaluation of the selection process may vary from one organization to another.

The selection criteria are:

1. The physical ability of the employee
2. The number of employees who will be available at the office on daily basis
3. The job description of the employee

The physical ability of the employee does not mean that a specific employee will not be trained. It means the employee may be tasked with an activity that he/she is capable of doing.

For example, an employee may not have the physical ability to stand at the facility gate, but he/she can be trained to operate the CCTV system.

The number of employees that will attend the security training depends on the total number of the employees available against the number of the required security employees. For example, when the number needed is 10 employees, the organization may need to train 20 or more taking into consideration the rate of authorized and unauthorized absence.

The original nature of the employee's job is an important factor to consider. For example, the company physician must stay at all time in his office especially in case there is disruption.

In addition to all of the aforementioned training criteria, there must be a training schedule of refreshment courses to the employees. Then, there must be an update of the training material in the event that one of the security processes has been replaced. In addition, when there is new security equipment, the training program must be updated to include the relative training on the new equipment.

PERFORMANCE KPI

After creating of the risk register, designing of the contingency plans and training the employees, the organization needs to make sure that the security system will be able to perform the required processes in the event of disruption[1, 6, 8, 10, 12, 18, 19, 20, 21, 22]. Therefore, the organization must develop an evaluation protocol to measure the system performance.

Just the same as the evacuation drill, the company may schedule security drills. Some of these exercises may be on quarterly basis and announced to the employees, and there can be one unannounced exercise per year. Those exercises, when measured, will help the organization to assess the ability of the organization to carry out the security services in case of disruption.

MEASURING SECURITY SERVICES SCR KPI'S

Though the aforementioned KPI's may vary from one organization to another and from one supply chain model to another, the most important part remains to be how to measure those KPI's. The organization needs a numerical model to assess the resilience of its security system. Thus, when the resilience improves, the organization can identify how well the system resilience improved and set accurate improvement targets to the security department.

This research paper proposes using reliability to measure the preparedness and performance of the security services supply chain resilience initiative[13, 14, 23, 24, 25, 26]. For this purpose, the paper proposes some evaluation criteria for the assessment. In addition, the research proposes numerical values for each criterion. The proposed numbers for the criteria may vary according to several factors such as the supply chain model, the organization selection of different business coefficients, and the nature of the business of the organization. Furthermore, the security services supply chain resilience level will be the product of preparedness KPI multiplied by the performance KPI as the two KPI's represent a series model. That is,

$$SCR = \Pr_R \times Pe_R \quad \textbf{(1)}$$

Where SCR represents the supply chain resilience, Pr_R represents the preparedness reliability, and Pe_R represents the performance reliability.

MODELING THE PREPAREDNESS KPI

To measure the reliability of the security services SCR, the organization will decide upon the criteria of evaluation and use one of the methods or techniques to transform those criteria into weighted values. Thus, the organization will convert the criteria into numerical data. The numerical data will easily fit in the reliability model. Using the binary system, the values given will be either 0 or 1, where 0 means available and 1 means is not available. This will be applied to all entries of the risk register, contingency plans viability, and the employees' training.

The proposed risk register criteria and values are in table 2. For the purpose of this research, table 1 entries will be used as example.

Table (2) Preparedness Reliability Evaluation

Criteria	*SR1*	*SR2*	*SR3*
1. Up-to-date (within the last quarter)	1	1	1
2. Has at least one viable contingency plan	1	1	1
3. The contingency plan has its owner	1	1	0
4. Employees are trained to perform contingency plan	1	1	1
5. The contingency plan approved by the top management	0	1	0
6. Monitored and controlled	1	1	1
7. SR Reliability	0.833	1	0.667

The reliability of the risk register will be,

$$RR_R = SR1_R \times SR2_R \times SR3_R \quad \textbf{(2)}$$

Where RR_R is the Risk Register Reliability, and SRN_R is the reliability of each identified security risk and N is the number of the identified risks. SRN_R equals the sum of all values divided by the number of criteria.

$$RR_R = 0.556$$

For the purpose of this research, the reliability of the contingency plan viability and training were entered as values 2 and 4 of table 2. However, the organization may decide to

establish a separate table for each one of them with its own criteria guided by the criteria given in this research.

MODELING THE PERFORMANCE KPI

For measuring the performance, the organization will track the execution of security processes conducted by the trained employees during the security exercise proposed earlier. In addition, the organization may assume the equipment maneuver plan as in the incident of the CCTV. The organization may assume that security employees went on a strike and the CCTV system has 5 defective cameras (the cameras can easily be disconnected or shut down). Then, the company will count the number of processes performed properly and the ones that were not performed. The performed process will take 1 and failure will take 0. The results of the exercise are indicated in table 3.

Table (3) Performance Reliability Evaluation

Criteria	*Number Attempts*	*Number Success*	*Reliability*
1. Performing personnel scanning for weapons at entry	20	17	0.85
2. Retrieving Video from CCTV system	10	8	0.8
3. Registering facility entrants	20	19	0.95

$$Pe_R = C1_R \times C2_R \times C3_R \quad \textbf{(3)}$$

Where CN_R is the reliability of each criterion as N is the given number of criteria.
The result:

$$Pe_R = 0.85 \times 0.8 \times 0.95 = 0.646$$

SECURITY SERVICES SUPPLY CHAIN RESILIENCE REPORT

This is a sample report that concludes the security services supply chain results and actions required to improve resilience levels.

Current resilience level is $SCR = \Pr_R \times Pe_R = 0.556 \times 0.646 = 0.359$

Recommended actions to improve SCR include (before the next security exercise):

1. Identifying all the owners of the risk register contingency plans.
2. Acquiring the approval on all the contingency plans in the risk register
3. Conducting a crash course to the employees assigned to operate CCTV system

CONCLUSIONS

This research paper introduces a reliability model for measuring the resilience KPI's of security services supply chain. To achieve that result:

(1) The research introduces three proposed models for security services supply chain.

(2) The research identifies two KPI's to measure the security services SCR.
(3) The research proposes reliability models to measure SCR KPI's.
(4) The research recommends that organizations attempt to apply the proposed models to acquire better security services capable of facing future uncertainties.

ACKNOWLEDGMENTS

I would like to extend my sincere appreciation to my family for their tolerance while I was working on this research. I would like, in addition, to thank Dr. Samer Farghaly, Dr. Abd ELAziz Mohamed and Dr. Mohamed Zaki for their insights on the content of the research. I am also much obliged to Dr. Engy Arafa and Ahmed Samy for their support and timely response in editing this research. Finally, I would like to thank my colleagues Khaled Alam Eldin and Sherif Ahmed for their insights over the research work as security experts.

REFERENCES

1. Fagel, Michael J., *Crisis Management and Emergency Planning: Preparing for Today's Challenges*, CRC Press, Taylor & Francis Group, 2014.
2. Márquez, Adolfo Crespo, *Dynamic Modelling for Supply Chain Management: Dealing with Front-end, Back-end and Integration Issues*, Springer, London, 2010.
3. Remigio, Helena Maria Lourenço Carvalho, *Modelling resilience in supply chain*, PHD Dissertation, Nova De Lesboa University, Portugal, 2012.
4. Southworth, Frank, Hayes, Jolene, McLeod, Shannon, and Strauss-Wieder, Anne NCFRP, Report 30, *Making U.S. Ports Resilient as Part of Extended Intermodal Supply Chains*, National Cooperative Freight Research Program, Transportation Research Board 2014 Executive Committee, Washington, D.C., 2014.
5. ASIS International, *Facilities Physical Security Measures: Guideline*, ASIS GDL FPSM - 2009, An ASIS Guideline for Security, American National Standard Institute, Inc.
6. ASIS International, *Business Continuity Management Systems: Requirements with Guidance for Use*, ASIS Spec. 1-2009, American National Standard Institute, Inc.
7. ASIS International, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*, ASIS Spec. 1-2009, Organizational Resilience Standard, American National Standard Institute, Inc.
8. Queensland Health, *Guideline for Security Risk Management and Asset Protection: Statewide Distribution*, Queensland Government, 2012.
9. Ikerd, John e., *Crisis & Opportunity: Sustainability in American Agriculture*, University of Nebraska Press, Lincoln and London, USA, 2008.
10. Cole, Jennifer, *Measuring the Resilience of Cities: The Role of Big Data*, Proceedings of the Conference Measuring the Resilience of Cities: The Role of Big Data, USA, 25 October 2013.
11. Blyth, Michael, *Business Continuity Management: Building an Effective Incident Management Plan*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009.

12. Business Continuity Institute, *Business Continuity Management: Legislation, Regulation and Standards*, Version 7, January 2012.
13. Leemis, L., *Reliability: Probabilistic Models and Statistical Methods*, Prentice-Hall, Englewood Cliffs, New Jersey, 1995.
14. Farghaly, W., Mohamed, Abdelaziz, *Using Reliability Models to Improve Security Systems' Performance at Minimum Cost*, International Maritime Transport & Logistics Conference (MARLOG 3), 2014.
15. Lynch, Gary S., *Single Point of Failure: The Ten Essential Laws of Supply Chain Risk Management*, John Wiley & Sons, Inc., Hoboken, New Jersey., 2009.
16. Zsidisin, George A., Ritchie, Bob, *Supply Chain Risk: A Handbook of Assessment, Management, and Performance*, Springer, 2009.
17. Waters, Donald, *Supply Chain Risk Management: Vulnerability and Resilience in Logistics*, The Chartered Institute of Logistics Management, Kogan Page, London and Philadelphia, 2009.
18. International Labour Organization, *Multi-hazard Business Continuity Management: Guide for Small and Medium Enterprises*, ILO Programme for Crisis Response and Reconstruction (ILO/CRISIS), 2011.
19. Gallagher, Michael, *Business Continuity Management: How to Protect Your Company from Danger*, Prentice Hall, Pearson Education Limited, 2003.
20. Hampton, John J., *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposures, and Seize Opportunities*, American Management Association, USA, 2009.
21. U.S. Department of Justice, Operation Partnership: Trends and Practices in Law Enforcement and Private Security Collaborations, Office of Community Oriented Policing Services, 2005.
22. Hiles, Andrew, *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons, Ltd, 2007.
23. Stratton, W., *Accounting Systems: The Reliability Approach to Internal Control Evaluation*, Decision Sciences 12 (1): 51-67, 1981.
24. Srinidhi, B., and Vasarhelyi, M., *Auditor Judgment Concerning Establishment of Substantive Tests Based on Internal Control System Reliability*, Auditing: A Journal of Practice and Theory 19(1): 1-16, 1986.
25. Mohamed, A., Qureshi, M.A., & Behnezhad, A.R., *Reliability and Design of AICS: A Survey of Models and Experiments, Review of Accounting and Finance*, Volume 4, Number 2, 2005.
26. Boronico, J. S., *Postal Service Pricing Subject to Reliability Constraints on Service Quality*, Pricing Strategy and Practice, Volume 5, Number 2, pp. 80-93, 1997.