BARRIERS OF ISO28000 SUPPLY-CHAIN SECURITY-STANDARD

Simon Julius Funken
ESB Business School, Reutlingen University, Germany

Shahryar Sorooshian
Faculty of Industrial Management & Centre for Earth Resources Research and Management, Universiti Malaysia Pahang, Malaysia

ABSTRACT

This research aimed at investigating the barriers that influence implementation of security standards and security management systems in industry. For this purpose, a list of barriers was established from analysing journal articles and books, using narrative literature review. The journal articles and books investigated other ISO standards due to the lack of literature on security standards, ISO28000. A list of 17 barriers was identified. Since there is no list of barriers of implementing security standards and security management systems to be found in the literature, the established list fills a gap in research. The findings of the study can be used in future research to investigate ways to lift the industries by reducing the barriers to, and highlighting the importance of, security standard certification.

Key words: Barriers, Industry, ISO28000, Security Standards.


1. INTRODUCTION

The International Organisation for Standardisation established the ISO28000 standard in 2005 in its first edition ISO/PAS 28000:2005. This version was revised in 2007, which is the standard currently in use. The above mentioned standards are specifically designed to focus on one aspect of security management whereas the ISO28000 encompasses a more holistic approach covering more requirements [1]. Several fields of supply chain security management like financing, manufacturing, information management, transportation, and warehousing are incorporated in the standard [2]. The aim is to implement, improve, maintain, and establish an organisation’s security management system [2,3]. The main advantage of ISO28000 in comparison to other supply chain security standards is the two-level view, focusing on the operator as well as the supply chain level. It is the only standard that allows for this level of security assurance [4].
Due to the nature of the supply chain as a combination of constantly evolving activities and processes, the ISO28000 standard follows the Plan-Do-Check-Acts (PDCA) cycle to accommodate the requirements of the supply chain [5]. ISO14000:2004 was used as a template for the format of ISO28000. Both standards incorporate a risk based management system approach which enables a wider application in terms of company size from small to large as well as every stage of the supply chain, starting from the sourcing and raw materials to final delivery. The standard can be used in two ways, either as a basis to implement measures to form a supply chain security management system or as a checklist to show compliance of an existing system and proof of compliance to third parties. The standard is divided into five main [5]:

1. Security management policy
2. Security risk assessment and planning
3. Implementations and operations
4. Check and correct action
5. Review and continual progress.

The first clause defines that an organisation seeking ISO28000 certification must ensure that the efforts towards enhanced supply chain security are supported by top management and that the general organisational structure is in place. A high level of transparency and visibility is desired so that all stakeholders have access to clearly defined security management objectives. Coming back to the PDCA cycle, the objectives should be aligned with the organisation’s size and nature and aim for continuous improvement [6].

The risk based management approach lies special importance on the second clause of security risk assessment and planning. Its main objective is to ensure a comprehensive view of threats related to security breaches that could affect an organisation. ISO28000 tries to achieve this objective by assessing an event’s likelihood and the consequences resulting from it. The events that could happen are divided into internal and external threats to the organisation. Internal threats incorporate intentional and unintentional failure of assets and resources, where external threats consider natural events such as floods and storms, which are not controllable by the organisation, as well as third party service and equipment failure [5].

Documentation and legal advisory are crucial elements of the implementation of ISO28000. Procedures must be in place to ensure access to legal and security regulatory requirements. The documentation must be relevant, achievable, measurable, and specific and should contain the security management programs, objectives and targets. Communication throughout all levels of the organisation must be enabled to provide the highest level of security possible [6].

The following clause, implementation and operation, deals with practical considerations, specifically mentioning the structure, responsibilities, and authorities of the workers. In order to successfully implement the security standard, properly trained staff have to be in charge and necessary resources must be allocated accordingly. Similar to the previous clause, communication is an important element. All stakeholder should be able to obtain information appropriate to their level. The same principle applies to the documentation and data control. Confidentiality and relevance of information to authorised stakeholders is key. Based on the PDCA cycle, the documents should be reviewed and revised on a regular basis [5].

Checking and corrective actions proposes monitoring and evaluation of the implemented security system. The organisation has to ensure that procedures are installed that can monitor quantitatively and qualitatively. The performance of meeting set targets and objectives must be monitored and the quality of the monitoring actions must be periodically reviewed and evaluated. The continuity of the security systems must be kept in check through regular audits.
in order to detect variation from the security standards and execute immediate counter actions to ensure compliance with ISO28000 [5, 6].

The last clause defines the role and responsibilities of the top management. High level conformity of the implemented security system with the organisation’s strategic plan and objectives has to be reviewed and if necessary changes in the security management system’s policy must be considered. This review requires documentation from all prior clauses and all levels within the organisation [5].

Derived from the last preceding paragraphs, CTPAT, TAPA, CSI and ISPS are rather specified security standards, each focusing on one part of the supply chain. ISO28000 on the other hand establishes a more comprehensive idea of a security management system. Despite this holistic approach, ISO28000 is not commonly used in the industry. According to a survey [7], only 356 companies worldwide are ISO28000 certified. In comparison to the most popular standards ISO14001 and ISO9001 which account for 1.1 million and about 350,000 accredited companies respectively, ISO28000 is the least accepted and implemented standard developed by ISO. Industry wise ISO28000 is mainly used in the construction sector with a total of 116 certifications, followed by other services and transport, storage and communication presenting 47 and 20 certifications respectively. Most of the certified companies can be found in Europe and specifically in Hungary, where 149 certifications were accredited in 2016 [7].

2. BARRIERS OF IMPLEMENTING ISO AND SECURITY STANDARDS

High investment cost is in all studies looked at a major reason for not implementing a new standard. Additional equipment and process changes require companies to make a budget available that can be used without having a direct payback of any form. Mariotti et al. [8] even found that some companies had stopped the certification process later on due to the high financial burden on the company. The investment cost must also be seen in connection with the barrier “no expected or perceived advantage”. Profit-driven companies have to consider whether the investment is worth it and if the benefits drawn from it will outweigh the costs. Santos et al. [9] describe possible advantages such as improve employee awareness, respond to customer demand, and attaining corporate objectives and goals.

The following barrier concerning human resource practices and lack of skilled labour focuses on the distribution of information among the employees to understand the importance of certification and establish incentives and rewards that are aligned with the overall company policy and objectives. Mariotti et al. [8] highlight the problem of a lack of specialists in the field of the security management that can hinder the efforts to achieve certification.

Top management commitment is seen as a crucial success factor for the implementation of a new standard by all three journal articles. The top management has to ensure that the pursued certification is in line with the company’s objectives and needs to communicate their support and endorsement to lower levels within the organisation. It encourages employees working on the implementation of the standard and makes discussions and political differences that may occur at a later point in time obsolete.

Missing encouragement, support and awareness of customer and missing awareness of supply chain members constitute two more barriers. If there is no demand from the customers or obligation from other supply chain members to implement standards, organisations will not gain any advantage from doing it. The need for certification must be identified by the organisation which can originate from either the customer, supply chain members, or regulatory pressure.

Luthra et al. [10] established in their paper “An analysis of interactions among critical success factors to implement green supply chain management towards sustainability: An
Indian perspective” critical success factors that can in turn also be seen as barriers in case they are not achieved. Apart from the ones mentioned in the previous paragraphs, three more are identified in their study. Missing organisation policy on the implementation of a standard is the first barrier, which is also endorsed by the International Organisation for Standardisation since it is one of the requirements for the implementation of ISO28000 under checking and corrective action [5]. The second additional barrier mentioned is a lack of information quality and sharing. This can also be found in the ISO28000 standard under security risk assessment and planning. Lastly, the third barrier is high cost for disposal of hazardous materials. This barrier is arguably not valid for all supply chain security management system but in regard to some resources, it is a considerable point that could lead to additional costs for the company.

Mariotti et al. [8] state eight more barriers in their study about barriers and benefits of implementing ISO14001 in Saudi Arabia. The amount of documents required in connection with the level of complexity of the documentation constitutes a major obstacle for companies due to the necessary resources that must be allocated to managing it and the time needed for preparation of documents. A poor legislative framework in the country the company is operating in linked with low pressure from the government to pursue certification were seen as further major barriers to implementing the standard. Missing guidance on how to implement the standard from the government hindered companies and encouraged a sceptical attitude towards it. The financial burden originated from the certification of ISO14001 manifested in a lack of incentives from the government, thus no financial support to assist in the implementation, and fees for auditing and external agencies to consult on the implementation constitute additional barriers for Saudi companies.

Although there is a gap in research on barriers of ISO28000, potential barriers for the standard implementation are listed based on a benchmark with ISO standards (e.g. ISO 14001 and ISO 9000). The table 1 shows the barriers of implementing ISO28000 which was derived from lists found in the literature. Verification of the validity of the listed barriers was with presentation and discussion of the list to experts of the field.

<table>
<thead>
<tr>
<th>#</th>
<th>Barriers</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High cost of investment</td>
<td>[8, 9, 11, 12]</td>
</tr>
<tr>
<td>2</td>
<td>Human resources practices and lack of skilled labour</td>
<td>[8-12]</td>
</tr>
<tr>
<td>3</td>
<td>Lack of top management commitment</td>
<td>[8-10, 12]</td>
</tr>
<tr>
<td>4</td>
<td>Missing encouragement and support from customers</td>
<td>[8, 11]</td>
</tr>
<tr>
<td>5</td>
<td>No expected or perceived advantage</td>
<td>[8, 9]</td>
</tr>
<tr>
<td>6</td>
<td>Missing supply chain member’s awareness</td>
<td>[8, 10]</td>
</tr>
<tr>
<td>7</td>
<td>Lack of information quality and sharing</td>
<td>[10]</td>
</tr>
<tr>
<td>8</td>
<td>High cost for disposal of hazardous materials</td>
<td>[10]</td>
</tr>
<tr>
<td>9</td>
<td>Missing organisation policy</td>
<td>[10, 12]</td>
</tr>
<tr>
<td>10</td>
<td>Missing pressure from government</td>
<td>[8]</td>
</tr>
<tr>
<td>11</td>
<td>Large amount of documentation required</td>
<td>[8, 12]</td>
</tr>
<tr>
<td>12</td>
<td>Poor legislative framework</td>
<td>[8]</td>
</tr>
<tr>
<td>13</td>
<td>Missing support/guidance on how to implement</td>
<td>[8]</td>
</tr>
<tr>
<td>14</td>
<td>Outdated legislation</td>
<td>[12]</td>
</tr>
<tr>
<td>15</td>
<td>No financial support to assist in implementation</td>
<td>[8]</td>
</tr>
<tr>
<td>16</td>
<td>Fees paid to registration/accreditation agencies for auditing</td>
<td>[8]</td>
</tr>
<tr>
<td>17</td>
<td>Required documentation is complicated</td>
<td>[8, 12]</td>
</tr>
</tbody>
</table>
3. CONCLUSIONS

Performance of Supply chain is crucial for companies [13,14]. A first step towards finding solutions and measures that can be implemented in order to improve the situation at the moment is to determine why companies are currently not much considerably implementing security standards for their supply chains. ISO28000 is the most holistic international standard available but worldwide not widely applied. Other standards are more commonly used and can shed light on the reasons to not implement security standards in the industry. Seventeen main barriers for the standard implementation found in this study; the barriers that can be subsequently used to investigate the motivation of companies to not implement ISO28000. The findings of this study give valuable insights to practitioners from the industry as well as legislators. Practitioners can use the established list to identify issues within their own organisation or, in case of certification agencies, to reduce hindering factors that influence companies when considering certification. Legislators can use the list to gain more understanding about the difficulties faced by companies that want to acquire standard certification.

ACKNOWLEDGMENT

This study thanks University Malaysia Pahang for flagship grant RDU172205.

REFERENCES


