
Pierre-Emmanuel Arduin¹, Doudja Kabeche² and Mustapha Sali¹
¹Université Paris-Dauphine, PSL Research University, CNRS, UMR 7088, DRM, Paris, France
²AgroParisTech, Paris, France
{firstname.name}@dauphine.fr
kabeche@agroparistech.fr

Abstract: In this paper, we argue that parallels can be drawn between information and knowledge systems security (IKSS) concerns of today’s organizations and quality management concerns of early twentieth century organizations. We propose a literature review of some Total Quality Management (TQM) and Lean Management (LM) solutions that may be relevant for information and knowledge systems security. This hybridization of IKSS and TQM/LM domains leads to propose innovative solutions for IKSS, notably by considering assignable causes and chance causes of security failures within organizations. Even if this work is still at an early stage, our approach suggests a shift from “security assurance” to “security control” within information and knowledge systems (IKS).

Keywords: Information and Knowledge Systems Security (IKSS), Insider Threats, Total Quality Management (TQM), Lean Management (LM).

1. Introduction

In our knowledge society, the mass computerization of information systems (IS) in the late twentieth century led to an explosive growth in information processed. The number of digital artifacts is constantly increasing. While yesterday a user was connected to a computer via a terminal, today the entry points for an IS are multiple, universal, interoperating and increasingly discreet. As a consequence, the number of associated possible uses (Canohoto et al., 2015) and ways of hacking (Mitnick, 2011) are also constantly growing.

As a resource, knowledge has to be shared within organizations to increase their ability to retain it (Liebowitz, 2008), as well as to create it (Nonaka and Takeuchi, 1995). Such statement led organizations to introduce IKS (Arduin et al., 2015), where individuals may easily share their knowledge, even if it cannot be made explicit. Authors as Watson et al. (2014) highlight how employees, who are as much knowledge-holders, may be hacked in organizations. Through manipulation techniques such as social engineering (Wilson, 2010), attackers may lead employees to share knowledge despite themselves: employees are then becoming an insider threat for the IKSS. In terms of knowledge management, we observed within organizations that not only (1) attacks may lead employees to share knowledge despite themselves by using manipulation techniques, but also (2) knowledge sharing may be a response to such attacks by raising awareness among employees. Such bilateral relationship between attacks and knowledge sharing will be discussed throughout this paper.

Quality, like security in today’s IKS, has gradually become a major managerial challenge in industrial systems in the wake of the Second World War. With the necessary reservations, analogies can be drawn between the dynamics that led to the emergence of the problems related to quality management in industrial systems and the issue of security in information and systems. In both cases, the multiplication of objects processed by technological and human resources in a context of increasingly complex processes with multiple inputs / outputs has contributed to the appearance of new threats in IS and new vulnerabilities in industrial systems. The maturity of the quality management approaches introduced during the second half of the 20th century suggests that a number of good properties resulting from this domain can be transposed to the IKSS especially with regard to the role of human agents that occupy a central place in both areas.

Indeed, we argue that insights can be gained from TQM and LM, two holistic approaches of quality management, to provide innovative solutions regarding IKSS concerns of today’s organizations. To identify relevant countermeasures against IKSS threats, we
propose an abduction procedure that consists to design concrete tools, solutions and devices suitable for information and knowledge systems security matters starting from the generic principles stated by TQM and LM. After remembering the vision of knowledge in the organization and the security approaches adopted in this work, a brief history of TQM and LM is presented. The research proposal is then explained and notably the ways a TQM or LM perspective may lead to innovative solutions for IKSS. This work is still at an early stage and the limits and perspectives for future works are finally discussed with the conclusions.

2. Background literature

The vision of knowledge in the organization adopted in this paper is introduced in the first part of this section. Security concerns related to such vision of knowledge in the organization are then presented in the second part of this section. The third part of this section sketches our research proposal by discussing a brief history of TQM and LM approaches, which will be used for proposing innovative solutions for IKSS.

2.1 A vision of knowledge in the organization

As the authors of this paper, we have got tacit knowledge, i.e. an individual cognitive construction, that we have structured into information during a process of sense-giving. As the readers of this paper, you have interpreted this information perceiving forms and colors, absorbed words, data, during a process of sense-reading, possibly creating new tacit knowledge for you (see Fig. 1). Sense-giving and sense-reading processes are defined by Polanyi (1967).

![Figure 1: Knowledge sharing: made explicit knowledge is transmitted and interpreted to create tacit knowledge (Arduin, 2015; based on Tsuchiya, 1993)](image)

Information is continuously interpreted during sense-reading processes. Within organizations, information can be transmitted by speaking, writing or acting, and also through IS. These communication media may be hacked, as well as employees themselves, in order to steal knowledge. Such knowledge can be:

- made explicit, i.e. it has been made explicit by someone within a certain context, it is socially constructed and can be supported by information technologies such as information. Individuals, as well as computers are “information processing systems” as said by Hornung (2009, p. 9),
- tacit, it is not always articulated and cannot always be articulated, relying on Polanyi (1958) notably: “we can know more than we can tell”.

So that made explicit knowledge is tacit knowledge that has been made explicit by someone within a certain context. It is information as a source of tacit knowledge for someone else. It is “what we know and can tell” answering to Polanyi (1958) quoted above. The term “explicit knowledge” is often used (by Nonaka and Konno, 1998, or Nonaka and Takeuchi, 1995, notably), whereas it does not reflect the dynamic of the sense-giving process as well as the term of “made explicit knowledge”. Indeed such process is attached to a certain person acting within a certain context. Attackers may target employees to steal knowledge by leading them to share it despite of themselves. Moreover, employees may engage in security policies violations on their
own. Now a few security concerns related to such vision of knowledge in the organization are going to be presented.

2.2 Security
The threats taxonomy proposed by Loch et al. (1992, p. 176) is worryingly topical even if we are twenty-five years after its publication (see Fig. 2). It suggests four dimensions of IS security: (1) sources, (2) perpetrators, (3) intent, and (4) consequences. Regardless of sources, perpetrators, and intent of an attack, consequences are nowadays the same: disclosure (of bankable information), modification or destruction (of sensitive information), and denial of use (by hindering access to resources). Such consequences are included in the norm ISO/IEC 27001:2013, information security management, which defines information security management systems as ensuring (1) confidentiality, (2) integrity, and (3) availability of information (ISO/IEC 27001, 2013).

Figure 2: Taxonomy of IS security threats (inspired from Loch et al., 1992)

Considering information and knowledge systems, the interpretative and cognitive component represented by employees has to be taken into account. Indeed cognitive processes as well as organizational contexts influence the violation of IS security policy by employees, who may become then users as attackers. According Willison and Warkentin (2013) employees’ violations of the IS security policy can be categorized in:

1. non-intentional, i.e. mistakes committed by careless or inexperienced employees, e.g. input errors, accidental deletions of sensitive data;
2. intentional but not malicious, i.e. deliberate actions realized by employees obtaining a personal benefit with no intention to harm, e.g. postponing backups, non-robust password choices, leaving doors open before a sensitive discussion;
3. intentional and malicious, i.e. deliberate actions realized by employees with the intention to harm, e.g. sharing sensitive data, introducing malwares.

While existing IS security studies have addressed how these violations of IS security policy occur, we argue that a TQM perspective may lead to innovative solutions for IKSS, such as a Total Security Management.

Moreover, workplace training and exposure provides knowledge to employees, allowing them to successfully violate IS security policy (Pahnila et al., 2007). The increasing complexity of security threat makes it difficult to anticipate, define and communicate all desired policy-compliant behaviors for all potential exceptions and circumstances. Now a brief history of TQM and LM approaches is going to be presented.

2.3 Total Quality Management and Lean Management
TQM is a management approach where the quality of goods and services produced is recognized as the main factor of long-term success for an organization. According to Ross (1993) and Yusof and Aspinwall (2000), TQM is a holistic management philosophy and set of practices that aim to ensure high-quality products and services to customers. For Kaynak (2003), TQM's objectives can only be achieved if the total quality concept is mobilized at each stage of the product or service life cycle.

Appeared in the vocabulary of managers and authors in the mid 1980s in the United States (Martinez-Lorente et al., 1998), the emergence of TQM as a management system is difficult to date precisely as its influences are numerous. Although the authorship of
the wording is still debated, the filiation of the concept is unanimously recognized in the works of Deming, Crosby, Feigenbaum, Ishikawa and Juran, which set out the main principles of the TQM in the 1940s (Powell, 1995; Walton, 1986). These quality gurus had the common idea of putting management at the service of quality by moving from quality insurance logics to integrated approaches of quality management at all levels (from design to consumption and production). The principles set out by these leading figures concerning the involvement of top management, the adoption of customer orientation, the supplier involvement, the employee empowerment and training, the continuous improvement of production processes, and benchmarking would be integrated, some decades later, under the banner of TQM.

Several authors have tried to unify and bring these principles together (Ahire et al., 1996; Flynn et al., 1994; Saraph et al., 1989). The following is a summary of the synthesis proposed by Martinez-Lorente et al. (1998), see Table 1.

To these principles of the TQM recognized and accepted by the majority of authors as the basis of a successful quality management approach (Kaynak 2003), positive externalities such as self-empowerment and the creation of a quality culture (Powell 1995) contribute to the success of this approach.

The first enterprise where TQM principles were applied in a holistic and systematic way is Toyota. The Toyota quality system is widely known as Toyota Production System, and has been labelled later as “Lean Management” by Womack et al. (1990). LM is related to the philosophy of achieving improvements in most economical ways with special focus on reducing muda (waste) (Dahlgaard-Park and Dahlgaard, 2006).

As said earlier, the main success factor for LM, and so for the TQM, is widely recognized as the employee involvement in following quality rules. Describing what they refer to as “the DNA of Toyota Production System”, Spear and Bowen (1999) have described the 4 rules, presented below, that can help practitioners to capture the tacit knowledge that underlies the TPS, see Box 1.

Table 1: Total Quality Management (inspired from Martinez-Lorente et al., 1998)

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top management support</strong></td>
<td>Top management commitment is one of the major determinants of successful TQM implementation. Top management has to be the first in applying and stimulating the TQM approach, and they have to accept the maximum responsibility for the product and service offering. Top management also has to provide the necessary leadership to motivate all employees.</td>
</tr>
<tr>
<td><strong>Customer relationship</strong></td>
<td>The needs of customers and consumers and their satisfaction have always to be in the mind of all employees. It is necessary to identify these needs and their level of satisfaction.</td>
</tr>
<tr>
<td><strong>Supplier relationship</strong></td>
<td>Quality is a more important factor than price in selecting suppliers. Long-term relationship with suppliers has to be established and the company has to collaborate with suppliers to help improve the quality of products/services.</td>
</tr>
<tr>
<td><strong>Workforce management</strong></td>
<td>Workforce management has to be guided by the principles of training, empowerment of workers and teamwork. Adequate plans of personnel recruitment and training have to be implemented, and workers need the necessary skills to participate in the improvement process.</td>
</tr>
<tr>
<td><strong>Employee attitudes and behaviour</strong></td>
<td>Companies have to stimulate positive work attitudes, including loyalty to the organisation, pride in work, a focus on common organisational goals and the ability to work cross-functionally.</td>
</tr>
<tr>
<td><strong>Product design process</strong></td>
<td>All departments have to participate in the design process and work together to achieve a design that satisfies the requirements of the customer, according to the technical, technological and cost constraints of the company.</td>
</tr>
<tr>
<td><strong>Process flow management</strong></td>
<td>Housekeeping along the lines of the 5S concept. Statistical and nonstatistical improvement instruments should be applied as appropriate. Processes need to be mistake proof. Self-inspection undertaken using clear work instructions. The process has to be maintained under statistical control.</td>
</tr>
<tr>
<td><strong>Quality data and reporting</strong></td>
<td>Quality information has to be readily available and the information should be part of the visible management system. Records about quality indicators have to be kept, including scrap, rework and cost of quality.</td>
</tr>
<tr>
<td><strong>Role of the quality department</strong></td>
<td>Quality department need access to top management and autonomy and also has to combine the work of other departments.</td>
</tr>
<tr>
<td><strong>Benchmarking</strong></td>
<td>A benchmarking policy for key processes should be in place.</td>
</tr>
</tbody>
</table>


Box 1: The 4 rules that can help practitioners to capture tacit knowledge underlying the Toyota production system (Spear and Bowen, 1999)

| Rule 1: All work shall be highly specified as to content, sequence, timing, and outcome. |
| Rule 2: Every customer-supplier connection must be direct, and there must be an unambiguous yes-or-no way to send requests and receive responses. |
| Rule 3: The pathway for every product and service must be simple and direct. |
| Rule 4: Any improvement must be made in accordance with the scientific method, under the guidance of a teacher, at the lowest possible level in the organization. |

As these rules cannot be made explicit, the only way to transmit them according to is to use a teaching and learning approach that allows workers to discover the rules as a consequence of solving problems. So, the fundamental pillar on which the performance of quality system relies is the workers involvement in learning process that increasingly gives deeper insights into their own specific work and makes them able to generalize how to design all activities according to the LM philosophy (Spear and Bowen 1999). Around these principles of both LM and TQM, have been developed a set of methods and tools which are used as countermeasures against different sources of waste and competitiveness loss (Statistical Process Control, Poka-Yoke, Andon, etc.). Beyond these tools, TQM and LM are above all holistic and integrative management philosophies based on a set of generic principles involving all the stakeholders (major functions of the company, top and middle management, operational staff, customers, suppliers, etc.) in a process of quality management in the broad sense (processes, products, services, etc.).

3. Research proposition: From “security assurance” to “security control”

The parallel we propose between the TQM/LM approaches and IKSS relies on two major justifications. First, the sufficient step back we have on the TQM/LM makes it possible to extract a certain number of lessons sufficiently generic to be transposed to other domains. Second, the holistic aspect of today’s security matters where human agents occupy a central place represent a strong similitude with early 20th century quality management issues.

Rather than attempting a direct transfer of the TQM/LM tools to solve the problems of IKSS, we propose to analyze the meaning that TQM principles could take in light of the challenges posed by IKSS. It will then be necessary to proceed by abduction, based on these principles, to devise concrete tools, devices and concrete recommendations for the IKSS.

To identify relevant countermeasures against IKSS threats, we propose an abduction procedure that consists to design concrete tools, solutions and devices suitable for information and knowledge systems security matters starting from the generic principles stated by TQM and LM. In this context, the tools of TQM/LM are considered as particular instantiations tailored for quality management. Equivalent tools remain to be defined with regard to the IKSS.

The implementation of this approach must be the subject of a full study that we do not intend to carry out here. However, it is interesting to illustrate this knowledge transfer between quality and security domains through a couple of examples. In order to adequately target the analogies to be exploited as a priority, we propose to analyze the origins of threats in information and knowledge systems through the framework proposed by Shewhart (1931) in the field of quality. We then illustrate through two examples the bridges that can be made between quality management tools and countermeasures against security threats in information and knowledge systems. We conclude this section by mapping some future research perspectives.
3.1 Security failure sources: Assignable causes and Chance causes

Inspection is the mean by which quality problems are revealed. Following Shingo (1986), there are three major inspection techniques:

1. Judgment inspection: Allows to separate defective products from good ones after processing (do not decrease company’s defect rate);
2. Information inspection: Inspects the causes of defects and have actions to try to avoid them in order to decrease company’s defect rate;
3. Source inspection: A defect is considered as the effect of a mistake. So, all mistake sources are put under control to avoid 100% of defects and tend to the “zero defect”.

It is the two later types of inspections that are in line with the spirit of TQM: Moving from product (or service) control to process control. Shewhart (1931) developed a frame to quality control by classifying these defect causes in two types: Assignable causes and Chance causes. Assignable causes are those whose effect can be detected and eliminated whereas chance causes (or common causes) are uncontrollable, due to random factors. Shewhart (1931) developed control cards to bring the chance cause variations in a controlled frame, to make them statistically predictable and controlled.

If we move from production quality control to IKSS concerns, we argue that the same frame can be mobilized to distinguish between security failures sources. Moreover, we argue that up to today, the approaches that are generally used to deal with this problem mostly address the assignable causes. It is the case for the approaches that consider the information and knowledge security matter through the risk management prism with tools as check-lists, passwords, rights of access, firewalls, traceability, etc.

We believe that we can go further and, move from “security assurance”, as supported by ISO/IEC 27001 (2013), to “security control” by developing tools and approaches that deal with chance causes of defects, i.e. chance cause of security failures. In the next section we will give examples of such tools.

3.2 Dealing with chance causes in information and knowledge systems security

We suggest to draw one’s inspiration from the approaches that have been developed with TQM and among them those which address chance cause sources of security failure. We distinguish between two kinds of tools: Statistical control tools (based on information inspection techniques) and systematic control tools (based on source inspection techniques).

3.2.1 Statistical process control (SPC) and Control Charts

SPC consists in monitoring the production process to prevent quality problems preventing from unusual or undesirable variation has occurred. The main tool supporting this approach are the control charts (see figure 3). They are devices where measures obtained from periodical sampling of production are plotted to see if they are comprised between control limits (namely upper and lower control limits). Since there are no sample points outside the control limits, most points are near the targeted average value and the point appear randomly distributed around the average (no growth or decrease of the values, not only from one side of the mean -above or less-) the process is considered “under control”.

![Figure 3: Illustration of a control chart](image)
Can we design control charts dedicated to IKSS management purposes? Let have a look at the philosophical pillars behind the control charts. The first pillar is to be able to translate a risk criteria (security failure) into a measure and to monitor the behavior (shape, variation, etc.) of a signal made by this measure between limits considered as an “acceptable” level of risk. Information and statistics about cyber attacks, number of spams in the mailboxes of employees, can illustrate the kind of signals to plot. It all depends on the correlation that has been made between the plotted variable and the security issue encountered. This is the second pillar on which the SPC relies: the scientific approach. Indeed, the design of control cards is not an ex nihilo construct. The continuous improvement process through the Plan-Do-Check-Act (PDCA) cycle approach for identifying causes of quality problems, and thus of security issues, are the spine of this approach. This leads us to stress again the importance of the employees involvement in the design of such approaches.

3.2.2 Systematic control tools: The Poka Yoke
Poka Yoke is the Japanese term for “mistake proofing”. It is any foolproof device or mechanism based on source inspection technique that prevents defects from occurring. It has been developed by S. Shingo as solution to the “Zero defect” ambition (Shingo, 1986). The idea underlying the Poka Yoke is to catch errors so they do not become defects. Poka Yoke addresses human errors in particular such as forgetfulness errors, misunderstanding errors, identification errors, lack of experience errors, willful errors, etc. (Shimbun, 1989).

Defect prevention is accomplished through the deployment of simple, inexpensive devises (see figure 4). “These devises are placed in the process to ensure that it is very easy for the operator to do the job correctly or very difficult for the operator to do the job incorrectly. The tool could be physical, mechanical, or electrical” (Denis, 2016).

As for the SPC control charts, TQM principles as PDCA cycle and employee involvement are key factors to the successful design, implementation and continual adaptation of the Poka Yoke to the quality system. We can easily draw a parallel between this quality tool and IKSS under concern in this paper. Indeed, human factor, as we pointed earlier is a major and not very well treated concern.

Figure 4: Illustration of a Poka Yoke

3.3 Discussion and future works
Despite the opportunities for closer links between security and quality issues, the literature proposing the application of TQM/LM approaches to the domain of IKSS remains very limited. This thematic rapprochement thus constitutes an opportunity for an original scientific contribution, which is started in this paper.

In a perspective closer to the one defended in this paper, Schiltz (2014) proposes a hybridization logic that aims at exploring the possibilities of transposing the TQM principles to respond to the security challenges in information and knowledge systems.
Considering security as an element of quality, Schiltz (2014) argues that integrating key components of TQM into security management can protect the availability, confidentiality, and integrity of information by securing people, processes, and technology on a social and organizational level. The tools and principles of TQM and LM, especially those related to continuous improvement and employee empowerment leading to a strong culture of ownership and accountability, are considered as relevant means to fight against security threats in information and knowledge systems. The ISO/IEC 27001 (2013) standard is an illustration of a tool dedicated to information security that makes the link with TQM principles. Indeed, ISO/IEC 27001 is an information security management standard part of the ISO/IEC 27000 family designed to help organizations to keep information assets secure. Security management is presented as a holistic risk management approach that rely, among all, on:

- Top management leadership and commitment;
- Integrated process management view;
- PDCA cycle of self-evaluation, correction and improvement;
- Employee awareness;
- Good practices documentation and generalization.

Adequate controls must be established within organizations to ensure, improve and control the security of information and knowledge systems. By involving everyone in all aspects of an organization, TQM leads to consider employees not only as sources of failures, but also as knowledge holders who have to be managed in order to secure the information and knowledge system.

4. Conclusions and perspectives

In a context of growing demand and competition pressure, companies adopted methodologies leading them to quality levels unattainable before. In the case of information and knowledge systems security, as quantities processed, as well as entry points are growing, the security approach and processes must be renewed to fit with nowadays challenges, such as insider threats leading employees to share knowledge despite themselves.

In this paper, we argue that IKSS, as an element of their quality (Schiltz, 2014), may be not only ensured, but also controlled through scientific methodologies inspired from TQM/LM. We began by remembering the vision of knowledge in the organization and the security approaches adopted in this work. Then we presented a brief history of TQM and LM. The research proposal has been explained and notably the ways a TQM or LM perspective may lead to innovative solutions for information and knowledge systems security. The perspectives of this work have finally been discussed at the end of this paper.

If authors as Stoneburner et al. (2002) argue that managing security risks has become less about quality and more about quantity, others as Schiltz (2014) defend that “integrating information security policies and best practice procedures through TQM will create a culture of informed and empowered employees holding information security as a top priority” (Schiltz, 2014, p. 22). The next step in our research is to deeply analyze the approaches that have been discussed in this paper. Specifically, we plan to: (1) Design countermeasures inspired from TQM/LM approaches through the abduction procedure illustrated in this paper; (2) Test them within industrial fields for information and knowledge systems security.

References


