Towards an Economic Approach to Identity and Access Management Systems Using Decision Theory

Eva Weishäupl, Michael Kunz, Emrah Yasasin, Gerit Wagner, Julian Prester, Guido Schryen, Günther Pernul
Department of Management Information Systems, University of Regensburg
{eva.weishaeupl, michael.kunz, emrah.yasasin, gerit.wagner, guido.schryen, guenther.pernul}@wiwi.uni-regensburg.de
julian.prester@stud.uni-regensburg.de

***Abstract*—Nowadays, providing employees with failure-free access to various systems, applications and services is a crucial factor for organizations' success as disturbances potentially inhibit smooth workflows and thereby harm productivity. However, it is a challenging task to assign access rights to employees' accounts within a satisfying time frame. In addition, the management of multiple accounts and identities can be very onerous and time consuming for the responsible administrator and therefore expensive for the organization. In order to meet these challenges, firms decide to invest in introducing an Identity and Access Management System (IAMS) that supports the organization by using policies to assign permissions to accounts, groups, and roles. In practice, since various versions of IAMSs exist, it is a challenging task to decide upon introduction of an IAMS. The following study proposes a first attempt of a decision support model for practitioners which considers four alternatives: Introduction of an IAMS with Role-based Access Control (RBAC) or without and no introduction of IAMS again with or without RBAC. To underpin the practical applicability of the proposed model, we parametrize and operationalize it based on a real world use case using input from an expert interview.**

Keywords*—*Identity and Access Management; Economic Decision Making; Information Systems; Information Security Investment; Decision Theory.

I. Introduction

Regulating access to resources, including systems and data, is a crucial challenge - in particular for firms which house and maintain sensitive and confidential information. According to the Ponemon 2014 Fourth Annual Benchmark Study on Patient Privacy & Data Security [1], malicious insiders, employee negligence, identity thieves and employee-owned mobile devices are four of the top 10 identified security risks. Taking this into consideration, employees' behavior, whether intentionally or unintentionally, poses a severe risk to information systems and contributes to the total of 5.6$ billion annual cost of such breaches for the surveyed U.S. health industry sector. Organizations have already started to implement specific measures to address the problem of internal attacks: The 2014 Insider Threat Report conducted by Ovum Research [2] states that Identity and Access Management (IAM) is one of the concepts most widely used in organizations in order to mitigate insider threats. Beyond their security effects, efficient IAM can significantly contribute to cost savings within a firm. Typically, medium to large-sized organizations manage hundreds of applications, ten-thousands of application accounts and millions of assignments of access privileges to their respective accounts. Hitachi, an Identity and Access Management System (IAMS) provider, estimates that replacing an inefficient application-centric user management by a structured state-of-the-art IAM in a large company can lead to cost savings of up to 2,100,100$ per year [3]. Such savings can be achieved through automated account provisioning and reduction of security administration efforts through an IAMS. In addition, regulations such as Basel III [4] and the Sarbanes-Oxley (SOX) Act [5] or other data protection and industry-specific acts such as the HIPAA [6] for the health care sector are playing an influential role for a company's IAM. By offering on-demand reporting of current access rights to resources, IAM supports compliance with such regulations.

While the advantages of IAMSs are obvious, some companies tend to only slowly adopt IAM due to the lack of management commitment. Executives are in favor of daily business which is why supportive functions - such as IT security in general - perceive strong attention only when incidents happen. The diffusion of RBAC, which replaces the inefficient design of ACLs, serves as an example to illustrate our point: missing or nontransparent economic evaluations of RBAC combined with high migration costs rarely lead to a kick off for projects required in order to replace old-fashioned access control models. However, the advantages of RBAC are obvious: As RBAC allows organizations to reduce access privilege assignments by bundling the privileges and grouping accounts into the respective roles, it enables a more efficient provisioning of new or updated user accounts. System administrators and helpdesk clerks are notably lifted off the time-consuming work of manually inspecting and assigning access rights.

In order to express how valuable an integration of IAMSs or the replacement of existing access control models is, we adopt a decision-theoretic based approach and formulate an economic model which supports decision makers whether to introduce an IAMS or not and whether to migrate to RBAC or not. We quantify the benefits of security and cost savings and take the firm's risk preference into account. By analyzing requirements from both research and practice, our contribution is to develop a model which can adapt company-specific parameters. Thereby we ensure real-world applicability of the proposed decision model.

The paper is structured as follows: In the next section, we provide a brief overview of the background and related work by reviewing the literature on IT security investments in general and on IAM in particular. In Section III, we develop and explain our decision support model with its components. Section IV underpins the proposed model by instantiating it based on a real world use case. Finally, in Section V we conclude our paper by summarizing the key results and give an outlook on future work.

II. Background and Related Work

Economic decisions concerning the investments of a company in an IAMS are often made in a similar context than decisions on investments in IT security in general. Several approaches to evaluating general IT security investments have been proposed in the literature [7], [8], most of which are either based on game theory or on metric development, such as Return on Security Investment (ROSI) [9]. However, as these models are defined on a more generic level of IT security investments, they have to be adapted or reformulated to provide adequate support for investment decisions in IAM. As stated by [10], the proposed frameworks and IT security investment models are not appropriate for deciding whether or not to invest in an IAM, as they do not reflect the wide range of potential benefits, in particular intangible aspects and the interconnectedness of the different aspects. Commonly used evaluation metrics for IT security investments ([9], [11]) are not easily applicable for economic decisions on introducing IAM. According to [12], [13], IAM projects comprise both operational and organizational aspects of the structure of an enterprise and therefore the level of complexity demands a broader scope. However, there are comprehensive models on how investments in IAM should be evaluated. The balanced scorecard based approach by [12] is one, which does not purely depend on financial parameters, but also includes managerial and organizational aspects. Beyond this approach, few studies have assessed the economic return of principal methods for managing users' access to information technology resources, e.g., RBAC. Both studies [14] and [15] assess the microeconomics of the benefits of RBAC relative to alternative access control systems. However, these approaches are highly dependent on many input parameters and therefore quite complex in evaluation.
Therefore, the following requirements for a decision support model for IAM investments can be identified:

- The decision support model should not only take into account monetary parameters, which would lead to single-dimensional and possibly sub-optimal decisions, as only an inadequate representation of the impact of investments in IAM is processed. Therefore organizational and managerial aspects have to be considered to take a comprehensive point of view.
- As executives tend to act in favor of daily business and disregard supportive functions like IAM, a decision support model has to be simple and fast in order to refrain from burdening decision makers in their daily workflows.
- The decision to invest in IAM depends on several factors. Therefore data collection and data quality always play a crucial role in comprehensive IAM approaches. Again, in order to facilitate a simple yet fast decision support model, it is necessary to exclusively require parameters, which are available to executive decision makers.

We have argued that there is a need to facilitate decision making in the domain of investments in IAM and to develop a simple and intuitive decision model to support decision making in the domain of investment in IAM. In order to be not overly dependent on unavailable parameters, we apply and extend the proposed evaluation of [15]. Therefore, contrary to extant research, the paper aims at closing the above mentioned research gap and explicitly considers an ex-ante view on IAM investments.

TABLE I. IAMS investment decisions under uncertainty

Actions	**States**			**Decision criterion**
	s_{low}	s_{med}	s_{high}	
$a_{IAM+RBAC}$	u_{11}	u_{12}	u_{13}	$f(u_{11}, u_{12}, u_{13})$
$a_{IAM+ACL}$	u_{21}	u_{22}	u_{23}	$f(u_{21}, u_{22}, u_{23})$
$a_{nIAM+RBAC}$	u_{31}	u_{32}	u_{33}	$f(u_{31}, u_{32}, u_{33})$
$a_{nIAM+ACL}$	u_{41}	u_{42}	u_{43}	$f(u_{41}, u_{42}, u_{43})$

III. Decision Support Model

In order to support decisions regarding the introduction of an IAMS either with or without an RBAC implementation, we adopt a decision-theory based approach. As can be seen in Table I, our proposed model consists of four mutually exclusive investment actions and three uncertain states, which correspond to different risks of attack. The rows in the decision model depicted in Table I display the four investment alternatives a decision maker has to decide on. Action $a_{IAM+RBAC}$ and $a_{IAM+ACL}$, respectively, represent the introduction of an IAMS with the introduction of RBAC or ACL. In contrast action $a_{nIAM+RBAC}$ and $a_{nIAM+ACL}$ define investment decisions without integration of an IAMS, again with implementation of RBAC or ACL. The columns in our decision model display the risk factor X. In detail, X defines the risk of attack a company wants to see itself protected against. We divide X into three intervals:

- Low: $X \leq 30\%$,
- Medium: $30\% < X \leq 70\%$,
- High: $X > 70\%$.

After calculating the twelve payoffs u_{ij} with $i = 1, ..., 4$ and $j = 1, ..., 3$, a decision maker can use criteria designed for decision making under uncertainty, e.g., the Maximin Criterion, the Minimax Regret Criterion or the Maximax Criterion [16], [17]. The chosen criterion depends on the firm's risk preferences. While the Maximin criterion takes a pessimistic or conservative risk attitude by assuming that the worst will happen [17], the Minimax Regret Criterion takes a sophisticated and comparative view on the decision alternatives. It tries to find the maximum regret over all states of nature for each decision and selects the decision alternative that has the minimum of these regrets [17]. The Maximax Criterion fits both an optimistic and an aggressive decision maker. This criterion is based on the best possible scenario exclusively [17].
In Section IV we exemplarily apply the Maximin criterion to a fictional use case.

The payoffs for different investment decisions and risks depend on different factors, such as cost, systems and applications of a organization. A tabular listing of all the variables used in our model, as presented in Table III, together with an

explanation can be seen in Table II. The model is based on the following assumptions:

- The deployment costs with RBAC integration Y_1 not only include costs for the technical installation of the IAMS product but also organizational costs, e.g., for modeling the roles. All four of the startup costs X_1, X_2, Y_1 and Y_2 are naturally dependent on the number of employees being managed in the IAMS.
- i_1 and i_2, respectively, define the percentage of potentially outdated or erroneously assigned access privileges to roles or direct access privileges. We assume i_2 to be significantly higher than i_1, as suggested by [18], because an ACL approach requires more complex administrative efforts.

After having defined the parameters of our decision support model, we can now devise the model itself. As indicated in Table III, we formulate a model, which comprises four possible actions, namely the implementation of an IAMS with RBAC or ACL and the introduction of RBAC or ACL without implementing an IAMS. For each of these four actions we calculate a payoff value u_{ij}. The payoff value depends on the model parameters we presented previously and the risk factor X. For calculation in our formulas we always use the upper boundary of the intervals of attack risks, in order to act on the assumption of a worst case scenario. However, the parameter X can be adjusted to match the decision makers attitude towards risk. In general the payoff formulas can be divided into three terms:
The first term of our formula contains the fixed costs X_1, X_2 and Y_1, Y_2, respectively. Exceptions are the payoff calculations for the scenarios with no IAMS integration. As our decision model should be particularly useful for firms which have not yet invested in IAM, we use the status quo of no IAM and ACL as a baseline and define the payoffs with regard to this baseline. The status quo obviously does not have any installation or deployment costs, but running costs for assigning access rights. When implementing RBAC, we at least have to include deployment costs, but still do not include installation costs. The fixed cost part is calculated through a sum over all installation and deployment costs.
The second term comprises the yearly costs, which are continuously incurred during business operations. We consider four standard activities in IAM and use weights and expenditures of time presented by [15]. The four activities are presented as:

- Assigning existing privileges to new users
- Changing existing users' privileges
- Establishing new privileges to existing users
- Terminating privileges

Each of these activities is assigned a rate, which quantifies how often the task appears in daily business. The rate is referred to as "Times per Employee, per Year" and its respective values for the sum are 0.20, 0.21, 0.20 and 0.17. The second parameter we adapt from [15], is the time necessary to complete the task for an administrator. Divided into "Time with ACLs" and "Time with RBAC", we multiply these values with the costs for the provisioning administrator. Values used for the "Time with ACLs" parameter are 12.4, 7.8, 9.2 and 7.6. The lower values for the "Time with RBAC" parameter are 6.9, 6.6, 8.0 and 4.7. The different coefficients result from time savings when RBAC is implemented. All values for the IAM tasks are scaled in minutes. The provisioning administrator's cost unit is given as $\frac{€}{h}$. Therefore the only variable part in the products is the number of employees and the provisioning admin's salary. In the calculation for our status quo we additionally multiply each task with the number of applications d, because each task has to be managed for each application and not only for one IAMS. Similarly, in case of an RBAC integration we also take into account all the applications, accumulate all users for each application and use the coefficients depending on whether RBAC is implemented into the specific application or not. The second term therefore expands to four sums over all applications d including the product of the number of accounts per application n and the provisioning administrator's costs multiplied by the period of time introduced above depending on whether RBAC is implemented or not, which is represented by r_n.
The last term of our formula includes measures for the risk preference of the firm. Therefore, we add the product of the the risk of attack factor X, the number of access privileges h and the cost in case of a security incident k. In case of an IAMS implementation we additionally include i_1 and i_2 respectively, to account for the rate of erroneous assignments of access privileges to roles or to concrete user accounts. We will show typical examples of these rates in the application of our use case in the next Section.

IV. Use Case

An use case has been carried out to explore the feasibility of the approach to providing strategic decision support for IAMS investments. To determine the necessary parameters for our decision model, we conducted an expert interview to gain practical information from real-world examples with industry-standard assumptions. Our exemplary company is a medium sized enterprise employing 5,000 people and it is planning to integrate four applications into an IAMS. The company assigned 1,500 access privileges in total. When using an IAMS with RBAC or without RBAC, respectively, we assume 5% or 20% of the 1,500 access privileges to be erroneously assigned, which is consistent with the findings of previous studies [18]. We choose both license costs and deployment costs to be equal regardless of whether RBAC is implemented or not. Therefore, we assume license costs of 50,000€ and deployment costs of 100,000€. For the administrator, who maintains the IAMS, we include the typical hourly wage of 45€. In case of a security incident regarding the IAMS, we estimate the attack costs to be 200,000€. Furthermore, our evaluation is based on an discount rate of 2%.
Using this fictional company we compute the following overall costs of our four possibly actions in the context of the three previously shown environmental states of assumed risk of attack factors of 30%, 70% and 100%. The results are depicted in Table IV.
After calculating the payoff table, we now use the Maximin criterion as a simple but effective criterion for decision making under uncertainty. This criterion is based on the worst-case scenario of each action. It fits both pessimistic and conservative decision makers. With regard to its computation, the Maximin criterion chooses the action that maximizes the minimum out-

TABLE II. MODEL PARAMETERS

Symbol	Parameter	Explanation
X_1	License fees for an IAMS **with** RBAC	This parameter takes into account the initial license costs of an IAMS. Industry experience shows that the licensing schemes of a majority of commercial IAMS are based on the number of managed identities. Prices vary from 10-25€ per identity.
X_2	License fees for an IAMS **without** RBAC	This parameter is equal to X_1, except that it takes into account the initial license costs of an IAMS without RBAC integration.
Y_1	Deployment costs for an IAMS **with** RBAC	This parameter includes all costs in conjunction with the installation of the IAMS. The fees depend on the number of employees, roles and applications.
Y_2	Deployment costs for an IAMS **without** RBAC	Almost identical to Y_1, this parameter represents deployment costs of an IAMS without RBAC integration.
c	Number of employees	c stands for the number of employees, whose identities will be managed by the IAMS.
a	Provisioning administrator costs	This parameter defines the hourly costs of the administrator, who performs the identity management operations within the company.
h	Number of access privileges	The parameter h characterizes the number of access privileges. h is necessary for both RBAC and ACL approaches, because the security incident severity is dependent on the number of access privileges being affected.
j	Discount rate	The discount rate j refers to the interest rate used in discounted cash flow analysis to determine the present value of future cash flows in our decision model.
k	Estimated cost in case of a security incident	k takes into account the cost that are incurred by an insider attack.
i_1	Rate of erroneously assigned access privileges to roles	This parameter defines the rate of access privileges of the IAMS with RBAC, which have been assigned to their respective users incorrectly.
i_2	Rate of erroneously assigned direct access privileges	This parameter is equal to i_1, except that it shows the rate of erroneously assigned privileges on an ACL basis.
d	Number of applications	The parameter d includes the number of applications, which will be integrated into the IAMS. Each of these applications will be described in more detail with the next two variables.
e_n	Number of accounts per application n	e_n describes for each application n the number of accounts, which are actively using the application. As mentioned earlier, we assume e_n to be equal to c for most of the applications, which will be integrated into an IAMS.
r_n	Application support for application-specific RBAC	This last parameter is a binary variable and defines whether the application n supports RBAC or not.

come for every action. Therefore, we focus on the last column of our payoff table (Table IV), which represents the worst possible scenario with the highest rates of security incidents occurring. A decision maker with a pessimistic or conservative risk preference would make the investment decision based on the worst case scenarios with the highest risk of attack factor X for all four possible actions. Obviously, the highest risk of attack factor is associated with the highest costs of all three states. Out of these four available actions, a decision maker adopting the Maximin criterion would now opt for the integration of an IAMS with the implementation of RBAC, because this action would generate costs of approximately 16.1 million €, which is the least cost of all four actions.

V. CONCLUSION

The introduction of an IAMS is a complex task, as it has numerous impacts on the operational and organizational structure of an organization. Therefore an analysis of the relevant aspects has to be taken into account in a comprehensive decision support model. With regard to the available data and a focus on simple and fast calculation, our approach can serve as an orientation rather than a complete decision support model. Although our model includes only parameters, which are available in most cases, the decision maker has to have a clear understanding of these variables and what they imply in the context of the particular company. Our proposed model is not suitable for every aspect of decision making in IAM. Since it does only include the provisioning aspects of an investment decision in the field of IAM, we aimed at fast and real-world applicability of the model. Another limitation of our decision support model might be that it mainly depends on monetary parameters, which could lead to sub-optimal results. However we included the decision makers willingness to take on risks and just converted it to a financial indicator in order to establish comparability.

This paper presents a systematic decision support framework for the introduction of IAMS into organizations. We formulated a decision theory based approach working with typically available model parameters. Therefore we first quantified the

TABLE III. DECISION SUPPORT MODEL

Actions		**Cost** (depending on $X = 30, 70, 100$)
with IAMS	RBAC	$X_1+Y_1+\frac{1}{j}[0.2\cdot c\cdot 6.9\cdot\frac{a}{60}+0.21\cdot c\cdot 6.6\cdot\frac{a}{60}+0.2\cdot c\cdot 8\cdot\frac{a}{60}+0.17\cdot c\cdot 4.7\cdot\frac{a}{60}]+X\cdot h\cdot i_1\cdot k = u_{1p}, p = 1,2,3$
	ACL	$X_2+Y_2+\frac{1}{j}[0.2\cdot c\cdot 12.4\cdot\frac{a}{60}+0.21\cdot c\cdot 7.8\cdot\frac{a}{60}+0.2\cdot c\cdot 9.2\cdot\frac{a}{60}+0.17\cdot c\cdot 7.6\cdot\frac{a}{60}]+X\cdot h\cdot i_2\cdot k = u_{2p}, p = 1,2,3$
without IAMS	RBAC	$0+Y_1+\frac{1}{j}[0.2\sum_{n=1}^{d}(e_n\cdot\frac{a}{60}((12.4-6.9)r_n+6.9))+0.21\sum_{n=1}^{d}(e_n\cdot\frac{a}{60}((7.8-6.6)r_n+6.6))+0.2\sum_{n=1}^{d}(e_n\cdot\frac{a}{60}((9.2-8.0)r_n+8.0))+0.17\sum_{n=1}^{d}(e_n\cdot\frac{a}{60}((7.6-4.7)r_n+4.7))]+X\cdot h\cdot k = u_{3p}, p = 1,2,3$
	ACL	$0+0+\frac{1}{j}[0.2\cdot c\cdot d\cdot 12.4\cdot\frac{a}{60}+0.21\cdot c\cdot d\cdot 7.8\cdot\frac{a}{60}+0.2\cdot c\cdot d\cdot 9.2\cdot\frac{a}{60}+0.17\cdot c\cdot d\cdot 7.6\cdot\frac{a}{60}]+X\cdot h\cdot k = u_{4p}, p = 1,2,3$

TABLE IV. USE CASE RESULTS

Actions		**States** X=30	X=70	X=100	**Maximin Criterion**
with IAMS	RBAC	5.6m €	11.6m €	16.1m €	**min(-5.6m €, -11.6m €, -16.1m €)=-16.1m €**
	ACL	19.5m €	43.5m €	61.5m €	min(-19.5m €,-43.5m €, -61.5m €)=-61.5m €
without IAMS	RBAC	92.8m €	212.8m €	302.8m €	min(-92.8m €, -212.8m €, -302.8m €)=-302.8m €
	ACL	95.4m €	215.4m €	305.4m €	min(-95.4m €, -215.4m €,-305.4m €)=-305.4m €

benefits of cost savings and security and we account for the risk preference of the firm. This model has been applied in an IAM use case involving a medium sized enterprise as a real-world example with common assumptions from the industry. Based on the presented research approach in Section III, the evaluation process and the decision-theory based assessment are a first step towards a decision support model, which is applicable to real-world IAMS investment decisions. However, future work is needed to extend the work presented here. We will evaluate different parameters, which work on a more generic level than the ones used in the current model. Nevertheless these new parameters have to fulfill the requirement of being easily applicable for the decision maker. With regard to our model, we will extend on the method how we integrate the risk factor into our calculation and evaluate more advanced approaches on how to measure the risk of attack. We also intend to implement the presented model into a prototypic software-based decision support system. The framework will allow decision makers to understand positive and negative impacts of the different input parameters when introducing IAM technologies into an organization.

ACKNOWLEDGMENT

The research leading to these results was supported by "Bavarian State Ministry of Education, Science and the Arts as part of the FORSEC research association (http://www.bayforsec.de/) and by the "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007-2013 (EFRE) as part of the SECBIT project (http://www.secbit.de).

REFERENCES

[1] Ponemon, "Fourth Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, Tech. Rep., 2014.

[2] O. Research, "2014 Vormetric Insider Threat Report (European Edition)," Ovum Research, Tech. Rep., 2014.

[3] Hitachi, "Example Savings Calculation - Hitachi ID Identity Manager," http://hitachi-id.com/identity-manager/savings/example.html - retrieved on 19-05-2015, 2015.

[4] Basel Committee on Banking Supervision, "Basel III - A Global Regulatory Framework for more Resilient Banks and Banking Systems," Bank for International Settlements, Tech. Rep., 2011.

[5] United States Code, "Sarbanes-Oxley Act of 2002," July 2002.

[6] U. D. of Health & Human Services, "Health Insurance Portability and Accountability Act of 1996," 1996.

[7] H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment," *Journal of Management Information Systems*, vol. 25, no. 2, pp. 281–304, 2008.

[8] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.

[9] W. Sonnenreich, J. Albanese, and B. Stout, "Return on Security Investment (ROSI) - A Practical Quantitative Model," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 45–56, 2006.

[10] D. Royer and M. Meints, "Enterprise Identity Management - Towards a Decision Support Framework based on the Balanced Scorecard Approach," *Business & Information Systems Engineering*, vol. 1, no. 3, pp. 245–253, 2009.

[11] J. vom Brocke, G. Strauch, and C. Buddendick, "Return on Security Investments. Towards a Methodological Foundation of Measurement Systems," in *Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007)*, 2007.

[12] D. Royer, "Assessing the Value of Enterprise Identity Management (EIdM) - Towards a Generic Evaluation Approach," in *Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES 2008)*, 2008, pp. 779–786.

[13] ——, "Enterprise identity management–whats in it for organisations," *Proceedings of the IFIP/FIDIS summer school on The future of identity in the information society*, pp. 403–416, 2008.

[14] G. Tassey, M. P. Gallaher, A. C. O'Connor, and B. Kropp, "The Economic Impact of Role-based Access Control," National Institute of Standards and Technology (NIST), Gaithersburg, MD, Tech. Rep. 07007.012, 2002.

[15] A. C. O'Connor and R. J. Loomis, "2010 Economic Analysis of Role-Based Access Control," National Institute of Standards and Technology (NIST), Gaithersburg, MD, Tech. Rep. 0211876, 2010.

[16] G. Perakis and G. Roels, "Regret in the Newsvendor Model with Partial Information," *Operations Research*, vol. 56, no. 1, pp. 188–203, 2008.

[17] R. Smith and B. Slenning, "Decision Analysis: Dealing with Uncertainty in Diagnostic Testing," *Preventive Veterinary Medicine*, vol. 45, no. 1, pp. 139–162, 2000.

[18] L. Fuchs, M. Kunz, and G. Pernul, "Role Model Optimization For Secure Role-based Identity Management," in *Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*, 2014.