



VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS
MASTER THESIS

Title of the Master Thesis: Leadership of High-Potential Security Talents

Author: Tobias Millauer, MA BSc

Matriculation number: h51822992

Program: PMBA Project Management

Supervisor: ao.Univ.Prof. Mag.Dr. Martina Huemann

© 2021 Tobias Millauer, MA BSc

Umschlaggestaltung: Buchschmiede

Druck und Vertrieb im Auftrag der Autorin/des Autors:

Buchschmiede von Dataform Media GmbH, Wien

www.buchschmiede.at

ISBN:

978-3-99129-261-6 (Paperback)

978-3-99129-260-9 (E-Book)



Das Werk, einschliesslich seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung des Verlages und des Autors unzulässig. Dies gilt insbesondere für die elektronische oder sonstige Vervielfältigung, Übersetzung, Verbreitung und öffentliche Zugänglichmachung.

Abstract

Professional MBA Project Management 2019-2021

Author of Master Thesis: Tobias Millauer, MA BSc
Title of Master Thesis: Leadership of High-Potential Security Talents

Supervisor: a.o.Univ.-Prof. Mag.Dr. Martina Huemann
Number of pages: 87
University: WU Executive Academy
Year: 2021

Companies are facing challenges due to shortages of skilled security staff. On the one hand, the security responsibilities of executive management and threats of attack are increasing, on the other hand, the market does not provide sufficient personnel for the labour force. The circumstances create extra workload on the existing security staff due to the risen number of responsibilities. Educated security staff is in the situation to select the employer and is able to choose from a wide range of companies. Recruitment of such highly demanded people requires specific treatment, as they understand their market value. In the course of this thesis, a mutual understanding between line managers, security personnel and the human capital department is reached by demonstrating mutual synergies and interdependencies. The incorporation of expert opinions on security talents enables new insights. The results confirmed the common picture in literature on high-potential security talents, however, the prevailing of the theories in practise depends on the respective organisation regarding financial appreciation and career opportunities. The applied leadership style has a direct influence on the willingness to continue working for the company. Future research should be conducted in the area of analysing the root causes of the pitfall situation based on the gaps identified in order to initiative structural improvements. Empirical data from quantitative interviews will underline the identified findings on high-potential security talents.

Table of Contents

Abstract	ii
1 Introduction	1
1.1 Relevance	1
1.2 Research Objectives and Questions	2
1.3 Research Design and Methods	2
1.4 Structure of the Thesis	9
2 Literature	11
2.1 Security in the Enterprise Context	11
2.2 Security Landscape and Threats	14
2.3 Human Resource Management (HRM) in the Context of Security	18
2.4 Identifying and Developing Security Leaders	26
3 Research Propositions	38
3.1 Critical Literature Summary	38
3.2 Structured Approach and Propositions	42
4 Empirical Part	44
4.1 P1: Market demand for High-Potential Security Talent	45
4.2 P2: Expected Compensation Packages of High-Potential Security Talents	47
4.3 P3: Career drivers of High-Potential Security Talents	49
4.4 P4: Relation between the Security Threat Landscape and Security Staff	51
4.5 P5: Distinction between Security Professionals and Security Leaders	53
4.6 P6: Appropriate Leadership Style for High-Potential Security Talent	55
4.7 P7: Effect of Talent Management Programmes for Security Professionals	57
5 Discussion	59
6 Conclusions and Recommendations	61
References	63

0 TABLE OF CONTENTS

A Sample Interview Questions	69
B Summary of the Interviews	70
B.1 Interview Partner 1	70
B.2 Interview Partner 2	72
B.3 Interview Partner 3	74
B.4 Interview Partner 4	76
B.5 Interview Partner 5	80
B.6 Interview Partner 6	84

List of Figures

1.1	Information Systems Research Framework	3
1.2	Conceptional Framework	4
2.1	Business Information Security Model	12
2.2	Current Cybersecurity Staffing & Level of Risk Caused by Staff Shortage	14
2.3	Fraud Rate of Austria	15
2.4	Security Incidents Evolution during 2017-2018	15
2.5	Persons prosecuted for Obstruction of Justice	16
2.6	Occurrence of Espionage by Province	16
2.7	Austrian Military Strategy and Threats	17
2.8	A Framework of strategic HRM in multinational Enterprises . . .	18
2.9	Talent Recruiting at the Austrian Intelligence Service	20
2.10	Recruitment Process	21
2.11	<i>“Teamwork Quality and the Success of Innovative Projects: A Theoretical Concept and Empirical Evidence”</i>	23
2.12	Interaction of Career Drivers and Outcomes	23
2.13	Intrapersonal Antecedents of Career Outcomes	24
2.14	Influence of the Psychological and Career Contract on Career Outcomes	25
2.15	Competence Atlas	28
2.16	HRM System in the Context of the Project-oriented organisation	29
2.17	Situational Leadership Model	30
2.18	Talent Management in the Context of HRM	33
2.19	Leadership Potential as a Framework for Measuring Future Capability	35
2.20	Talent Mgmt. Programme at a major Austrian Bank	36

List of Tables

1.1 Design Science Approach 4

2.1 Modes of Situational Leadership 32

A.1 Interview Questions 69

Acronyms

- BJA** Federal Chancellery of Austria. 74
- BMEIA** Federal Ministry for European and International Affairs. 81
- BMKÖS** Federal Ministry for Arts, Culture, the Civil Service and Sport. 74
- BP** Business Partner. 37
- CIO** Chief Information Officer. 7
- COO** Chief Operations Officer. 6
- CSO** Chief Security Officer. 37
- CSR** Corporate Social Responsibility. 19
- EMILYO** European Initiative for the Exchange of Young Officers. 6
- HC** Human Capital. 1, 2, 5, 11, 19, 36, 37, 39, 41–43, 45, 51, 52, 57, 60–62, 74
- HRM** Human Resource Management. 9, 18, 19, 26, 29, 33, 41, 42, 47, 69
- IAEA** International Atomic Energy Agency. 20, 21
- ICT** Information and Communications Technology. 46
- IDP** Individual Development Plan. 36
- ISMS** Information Security Management System. 74
- IT** Information Technology. 16
- MA** Master of Arts. 7
- MBA** Master of Business Administration. 6
- MSc** Master of Science. 6, 7
- MSD** Master of Security and Defence Management. 6

- OCM** Organisational Career Management. 25
- PBO** Project-Based Organisation. 29, 30, 37
- PESTLE** Political, Economic, Social, Technological, Legal, and Environmental.
19, 26
- PhD** Doctor of Philosophy. 6, 8
- POC** Project-oriented Companies. 41
- POO** Project-Oriented Organisation. 29
- SME** Subject Matter Expert. 34
- SSDLC** Secure Software Development Lifecycle. 19
- TMP** Talent Management Programme. 1, 2, 9, 33, 34, 36, 37, 43, 57, 69
- UAS** University of Applied Sciences. 7
- UN** United Nations. 20
- UNDOF** United Nations Disengagement Observer Force. 6
- WEGA** Wiener Einsatzgruppe Alarmabteilung. 7

Chapter 1

Introduction

1.1 Relevance

Companies across global industries must manage wide-ranging security risks that have to be managed appropriately. The expertise required to perform such complex tasks may not be available in the company or on the market due to skill shortages. No company can afford to neglect security within their products or services throughout the entire life cycle as it holds essential relevance and is indispensable for maintaining corporate reputation.

Top management has to fulfil their security requirements of different national and international laws as well as regulatory/industry standards. Of course, management itself is not in the position to implement security measures. They must assign the responsibility to respective security functions in order to ensure proper oversight and implementation. If the security function is not equipped with the necessary people, management might be exposed to liability risks.

The aim of this master thesis is to reach a common understanding between line managers, security professionals and the Human Capital (HC) department by demonstrating how security personnel should be lead. Security staff will be attracted from a suitable working environment which applies for hiring, promoting and retaining them. The employer's working environment is influenced by various factors such as a Talent Management Programme (TMP) that includes performance appraisals and promotions.

1.2 Research Objectives and Questions

The master thesis should offer line managers and the HC department the possibility to understand high-potential security talents and deduce how they must be managed from functional as well as hierarchical perspective. Management of security staff¹ implies leading, developing and promoting them based on their skills and potential. The research question of the master thesis is: *How should high-potential security talents be led?* Sub-research questions are defined to subdivide the main research question:

SRQ₁: *How does the market for security personnel and related risks look like, e.g. skill shortages?*

SRQ₂: *What expectations do security talents have in terms of their career?*

SRQ₃: *What profiles of security talents are able to lead others?*

SRQ₄: *How should a TMP for security personnel be designed?*

1.3 Research Design and Methods

The research design is based on the 4-D model² for business and management research [25] and contributes to the development research activity. The research theme is composed of the following dimensions: *context* (multinational companies), *discipline* (human resource management), *problem* (leading high-potential security talents) as well as *social group* (individuals and organisations).

The thesis is conducted in the area of social sciences and therefore draws on the ethnographic method with the inherent inductive logic. The research methods used are documentation analysis and interviews in order to ensure data viability. The qualitative research designs offers the possibility for a multidimensional iterative analysis of the research questions.

¹ Security staff is defined as people that work in the following domains regardless of the sector (private, public, military, research): information security, cyber/ICT/OT security, physical security, nuclear security, counter-terrorism, organised crime, corruption and economic crime, crime prevention and criminal justice as well as human trafficking.

² The 4-D model consists of 4 phases: D1 - Defining Research, D2 - Designing Research, D3 - Doing Research and D4 - Describing Research.

The design science in information systems research method [19] outlined in Figure 1.1 is used to answer the research question.

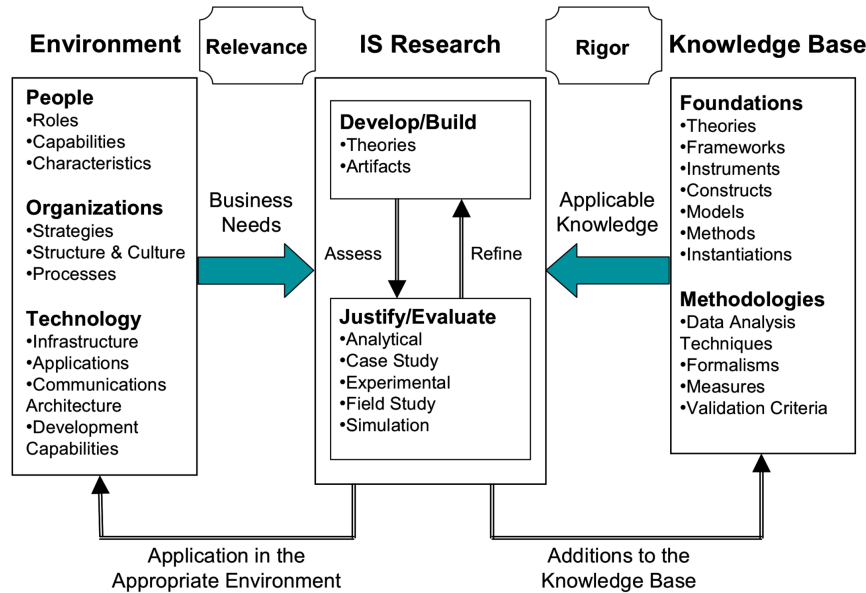


Figure 1.1: Information Systems Research Framework

Source: [19, p. 274]

First, a profound literature analysis was conducted to establish the foundation. *Second*, research propositions were made for preparing the empirical part. *Third*, expert interviews are performed in order to justify the research questions. *Finally*, conclusions and recommendations are drawn from the research findings.

Qualitative research data was collected via six semi-structured remote interviews, each one lasted about 45 minutes on average. The purposive sampling involves security experts in managerial position including disciplinary supervision from various industries presented in Section 1.3.2 *Interview Partners*. The interviews have been performed after the literature review and are based on predefined questions related to the research question listed in Appendix A *Sample Interview Questions*. The interviews were audio recorded with permission by the respective interviewee and transcribed in Appendix B *Summary of the Interviews*.

The thesis fulfils the design science guidelines as outlined in Table 1.1.

Design Science Guideline	Thesis	
	Chap.	Description
1. Design as an Artefact		Leadership of high-potential Security Talents
2. Problem Relevance	2.1	Security in the Enterprise Context
	2.2	Security Landscape and Threats
3. Design Evaluation	5	Discussion
4. Research Contributions	2.3	Human Resource Management (HRM) in the Context of Security
	2.4	Identifying and Developing Security Leaders
	4	Empirical Part
5. Research Rigour	2	Literature
	3	Research Propositions
6. Design as a Search Process	6	Conclusions and Recommendations
7. Communication of Research		Presentation at WU EA and a major Austrian Bank

Table 1.1: Design Science Approach

1.3.1 Literature Search

The literature search was conducted in the area of the conceptual framework outlined in Figure 1.2 with a mix of the keyword and snowball method.

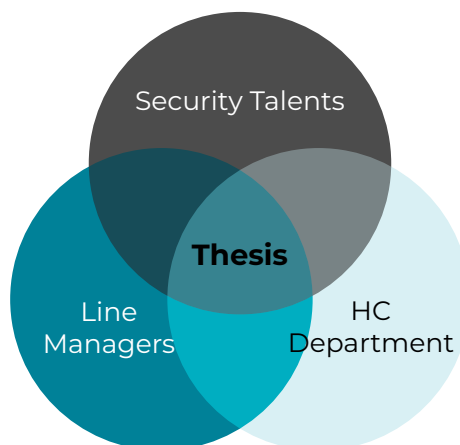


Figure 1.2: Conceptual Framework

The following significant databases were searched during the literature search:

- WU Catalog, <https://katalog.wu.ac.at/>
- Google Scholar, <https://scholar.google.com/>
- IEEE Explore, <https://ieeexplore.ieee.org/>
- Springer Link, <https://link.springer.com/>
- ElgarOnline, <https://www.elgaronline.com/>
- ProQuest, <https://www.proquest.com/>

The following keywords were used to obtain the literature results: *leadership, talent, security, career, management, risk, threat, fraud, military, espionage, cyber, recruiting, performance, 360-degree-feedback, skill, team, high-performance, development, challenge and sustainability*.

The literature holds high significance in the justification of underlying causes. The contribution to answering the research questions is given, as only highly qualitative information has been integrated into the thesis. The outcome of the literature review allowed systematic preparation for interviews because the interview participants could be asked relevant questions.

The research subject on the interconnection between high-potential security talent, line managers, and the HC department requires a literature analysis on each domain. The integration of the areas is reached by a mutual understanding of the specific peculiarities and the identification of commonalities, enabling new insight as results are brought together comprehensibly.

1.3.2 Interview Partners

Interview Partner #1

Interview Partner 1, Lieutenant General, was chief of the Swiss Armed Forces and reported directly to the head of the Federal Department of Defence, Civil Protection and Sport (DDPS). Since 2017, he has been involved in various foundation boards, is a special envoy of the Geneva Centre for Security Policy as well as a coach and trainer. *Interview Partner 1* studied business economics, attended the military school of the ETH Zurich and completed his Executive MBA at the University of Zurich.

Interview Partner 1 has over 40 years of leadership experience and knows how-to manage security talents as he had responsibility over 140'000 soldiers. The combination of economic and military background enables insights into the interconnected topic. He understands the development of response strategies, especially for emerging threats. A systematic approach for problem solving, as he applied during his career, is also a key component for evaluating high-potential security talents.

Interview Partner #2

Interview Partner 2 holds the professorship for comparative military leadership education of the Austrian Armed Forces and is chairman of the European Initiative for the Exchange of Young Officers (EMILYO) Implementation Group. Prior, he was the COO of the United Nations Disengagement Observer Force (UNDOF) in Syria. *Interview Partner 2* attended the Theresan Military Academy and holds an MSD from the National Defence Academy, both he graduated as best of class. He obtained an MSc in defence economy at the Corvinus University in Budapest, a PhD in security research from the Sigmund Freud University and an MBA in education management. With his Habilitation proceeding in Military Management at the University of Defence in Brno/Czech Republic he proofed evidence that international exchanges have positive effects onto Officer Cadets personal developments.

Training the new generations of leaders in the armed forces requires a deep understanding of socio-economic factors. In particular, the combination of international experience with the potential to lead others is propagated by *Interview Partner 2*. Interacting with the market for talents is a core competence to be attractive as a public employer.

Interview Partner #3

Interview Partner 3 is director of cyber security at the Austrian Federal Chancellery responsible for network and information system security, the coordination of nationwide cyber exercises and matters relating to the regulatory framework as well as the management of the Central Alternative Computing Centre of the Federation. Prior to his current position, he was CIO at the Austrian Constitutional Court. *Interview Partner 3* holds a MSc in Information Security Management from Danube University Krems.

Attracting talents in the public sector might be challenging as the compensation packages are mostly not on the same level compared to the private sector. Even more it is important, to generate and maintain a suitable working environment for high-potential security talents. *Interview Partner 3* provided insights into managing interconnected projects with security experts including supporting talents as well as understanding their career expectations.

Interview Partner #4

Interview Partner 4, Brigadier General, is Head of the Central Office for Combating Smuggling, Trafficking and Cross-border Prostitution at the Austrian Federal Criminal Police Office. He started his career as a police officer in Vienna, first serving with the special unit WEGA and later as a Criminal Investigation Officer. After his officer apprenticeship, *Interview Partner 4* was responsible for setting up the national Europol unit in Austria. He is a lecturer at various universities as well as international police academies and holds a MA in security management from UAS Wiener Neustadt.

Interview Partner 4 provided insights into the selection process of resilient security staff members that are able to cope with human destinies on a professional level. Dealing with people in the proper context is a decisive criterion for leadership competence. Moreover, he understands how-to keep the focus of his staff members into right direction over a long period of time until the complex and partly exhausted investigations are completed.

Interview Partner #5

Interview Partner 5, colonel of the General Staff Service, is Head of the Department for Information and Communication Technology Security and Cyber Defense at the intelligence service of the Austrian Armed Forces. Prior to his current role, *Interview Partner 5*, was also head of the electronical counterintelligence division. He completed the training for officers at the military academy in Wiener Neustadt and the 12th General Staff Course at National Defense Academy in Vienna. He is active in the security field for 30 years and has held more than 800 presentations on the subject.

Interview Partner 5 has the ability to manage high potential security talents by listening to their opinion and guiding them through the target to be achieved. Although the military is designed in a hierarchical way, he applies a cooperative leadership style to accomplish cyber missions.

Interview Partner #6

Interview Partner 6 is director of the institute of Criminal Law and Criminology at the University of Vienna as well as member of the university senate. The research focus is the law enforcement and protection of fundamental rights, responsibilities of the police and judiciary in criminal prosecution, computer criminal law and selected areas of economic criminal law. *Interview Partner 6* also was the deputy chairperson of the evaluation commission of the Federal Ministry of the Interior for the Natascha Kampusch case and is member of the Board advising the Minister of Justice in matters of ministerial instructions to be given to the prosecution authorities. *Interview Partner 6* holds a PhD in legal studies and is lecturer at various universities.

Interview Partner 6 understands how a research department with security experts must be led, especially researchers in terms of project performance and academic publications. Therefore, an essential part is the maintenance of an unbiased working environment without external influence for enabling objective results. The development of the next generation of researchers and supporting them on their career path is one main area of responsibility. An added-value for the thesis was the interpretation of the criminal landscape from a legal perspective.

1.4 Structure of the Thesis

Chapter 1: Introduction

The current chapter has outlined the relevance of the research, the objectives, the research questions as well as the research design including methods. The literature search criteria and the interview partners are also described.

Chapter 2: Literature

In this chapter, the literature consulted to perform the research is illustrated such as the security in the enterprise context and related threats. Human Resource Management (HRM) is analysed in regard to security for recruiting talents and creating the high-performance team. The identification and development of security leaders with a suitable TMP is likewise part of the chapter.

Chapter 3: Research Propositions

In this chapter, The critical summary of the literature acts as the foundation for the thesis in terms of research contribution. Each proposition is described and linked with the respective literature.

Chapter 4: Empirical Part

The qualitative interviews with the carefully selected experts are used to answer the respective research proposition in this chapter. Responses to the research propositions are supplemented by relevant citations.

Chapter 5: Discussion

The objective of this chapter is to provide a link between the theoretical literature analysis and the empirical data gained from qualitative interviews by highlighting research findings. The results are subject to interpretation.

Chapter 6: Conclusions and Recommendations

The conducted research is summarised in this chapter, the limitations are described, a further research agenda is outlined and potential effects are elaborated.

Appendix A: Sample Interview Questions

The sample questions used to perform the interviews are listed in this chapter with reference to the corresponding literature chapter and the research question.

Appendix B: Summary of the Interviews

In this chapter, the executive summary of each interview is provided as well as the date of the conduction.

Chapter 2

Literature

2.1 Security in the Enterprise Context

2.1.1 Introduction

The enterprise context of security will be demonstrated in this section to provide the background information to non-security people, especially top management and the HC department. The alignment of security terms to a common business language raises the understanding of the importance.

2.1.2 Security as a Business Enabler

The added value that security offers must be clearly communicated to executives by demonstrating security in the context of the enterprise and avoiding the consequences of neglecting potential drawbacks. Security leaders must understand how to transport key messages to top management and not only discuss them among other experts. Security does not exist for its own purpose; indeed, it supports the management in meeting their responsibilities and serves the respective business model.