Challenges and Competences in Master Degrees from a Comprehensive Security Perspective

Javier Espinosa García¹ , Luis Hernández Encinas^{1,2} ,
and Alberto Peinado Domínguez³

¹ Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), Madrid, Spain

{javier.espinosa, luis}@iec.csic.es

² Higher Technical School of Engineering (ICAI), Comillas Pontifical University, Madrid, Spain

³ E.T.S. Ingeniería de Telecomunicación, Universidad de Málaga, Málaga, Spain
apeinado@ic.uma.es

Abstract. Nowadays, the security threats faced by society in general, and organizations in particular, are reaching unprecedented highs in terms of complexity and sophistication. Organizations must face up to new challenges in order to protect their assets (e.g., personnel, goods, information, or reputation, among others), so they need new solutions for the immediate future to achieve their business objectives efficiently and effectively. Right now, corporate security and cybersecurity within organizations are dependent on themselves and complementary at the same time, so the coordination of their activities is crucial. This joint action for a comprehensive security requires a training and educational process that provides necessary knowledge and skills. This article highlights the limitations of the current master's degrees in cybersecurity from the perspective of comprehensive security and proposes a new master's degree focused on it as a solution, which takes advantage of the skills of current degrees, and is aligned with the needs of the European Higher Education Area. This master's degree promotes sustainability through efficiency and rationalization on the general asset protection process, improving the security culture inside the organization, reducing the number of security incidents, and increasing the reputation and image of the organization.

Keywords: Comprehensive security · Master's degree · Security education

1 Introduction

We are living in a digital and diverse society [1], so almost all human activities are threatened by a growing number of potential security risks [2], both physical and cyber. This shows that security controls to protect assets by removing or avoiding dangers or damages are crucial and significant.

Nowadays, nobody doubts that companies and institutions are increasingly becoming complex [3], both from an organic and functional point of view. Organizations move in a global and highly dynamic context where technologies play a decisive and crucial role. In fact, information is one of the key assets to protect within an organization and it

is commonly accepted that lies in electronic media that need to be physically protected, while the cybersecurity of the physical medium that contains the information must be guaranteed. These measures are interdependent and complementary [4]. In other words, it would not be possible to guarantee the cybersecurity of an asset without a suitable physical security, and vice versa. Terms such as integral, convergence, or fusion spread in the context of security, proving that physical and cyber security complements perfectly throughout their entire value chains, providing more benefits than drawbacks.

Comprehensive security (hereafter, CS) is a multidisciplinary concept aligned with current needs and trends [5, 6]. CS covers the most relevant fields of security, both strategic, tactical, and operational ones, aimed at preventing and avoiding any damage, danger or risk that threatens any asset for an organization. Of course, CS is a holistic process made up of procedures, techniques, and tools from heterogeneous nature such as scientific, technological, economic, financial, legal, or social, among others. CS is the natural response to current incidents that hit the organization assets, so much so CS transformation is still on progress. CS can be a challenge for any organization but generates efficiency advantages by eliminating duplicities and optimizing dedications and efforts.

Therefore, it seems necessary that those responsible for an organization security have a wider and solidier knowledge baseline that covers the whole CS scope [7]. Thus, a cybersecurity professional (e.g., a telecommunication engineer responsible for cybersecurity for an organization) should be fluent in methodologies and techniques specific to his traditional academic education and work experience, but also he should know and consider other areas or disciplines that will be essential for decision making under his responsibilities to organization activities. This paper brings an education proposal that tries to contribute to develop CS via a master's degree.

The rest of this paper is organized as follows: Sect. 2 describes a brief background about security and its approaches in organizations that leads to CS and gives rise to the proposed CS master's degree. Across Sect. 3, this paper presents the master's degree objectives and competences to be achieved by students, which adjust to the generic needs of current organizations with sustainability development requirements. In addition, during Sect. 3, this paper also presents the master's degree curriculum and program in terms of subjects, contents, and credits. Finally, Sect. 4 brings the main conclusions about the proposed master's degree in CS.

2 Comprehensive Security Background

Well into the 21st century, it can be somewhat accessory to arise the main reasons why individuals require security in any of their daily facets (e.g., personal, social, family, work, health, etc.). A security that, in general, is innate to human nature itself and that is closely related to the protection of needs and aversion to damage, both accidental and deliberate [8].

In this sense, until the middle of the 20th century [9], security consisted of the aspects of its physical component, fundamentally related to the protection of people (e.g., their life, health, and well-being, etc.) and the tangible assets of companies (e.g., buildings, machinery, goods, etc.). However, from the moment that electronic systems begin to develop in a generalized way and technological means begin to be incorporated into business processes, this traditional security concept has been modified and has been extended to new fields of action. It is not only about protecting the technology that automates production processes and lowers costs, but this technology has led to the recognition that also logical aspects must be protected, that is, business data, processed or stored in information systems, are tremendously valuable and are part of the intangible assets of the company [10].

This change in the conception of security has increased, even more, since new technologies are a constant feature and become a real part of the personal world, where the cyber aspects are highly critical. Therefore, the physical and logical aspects of security cannot be analyzed individually but must be considered jointly, since there are relationships and interdependencies between them that require a wider and more cohesive vision of the concept of security [11]. That is CS.

While regulated education is focused on cybersecurity [12], security [13] or safety management [14] as isolated topics, no university master's degree has been found (at least in Spain, according to the information on official master's degrees provided by ANECA [15]) by the authors of this work with a greater approach like CS. The analysis performed on master's degrees compliant with the European Higher Education Area (EHEA) framework, reveals that three main modules that define competences in cyber defense, cyberattacks and cybersecurity management support all of them.

3 Master's Degree in Comprehensive Security

A master's degree in CS (MCS) is presented as a proposal to overcome the gap detected in current cybersecurity master's degrees in the path to CS. MCS is twofold oriented, inasmuch as it intends that the students who complete it can either develop a doctoral thesis or pursue a professional career.

The very nature of the CS concept makes it neither necessary nor advisable to establish itineraries or specialties in the MCS. In this way, the MCS aims to cover the main topics related to CS from a global perspective.

All the MCS attendants will acquire training in all subjects related to CS with no compartmentalization nor distinction and MCS will prepare students for achieving professional certifications such as Certified Information Security Manager (CISM) from ISACA [16] or Certified Information Systems Security Professional (CISSP) from ISC² [17]. The MCS constitutes an extraordinary access path for multidisciplinary training and research in the CS field from a critical, respectful, ethical, and informed perspective.

3.1 MCS Objectives

The MCS, attending to the needs and trends of the security sector and the markets [18, 19], sets as its main objective the complete training of professionals in the most relevant fields of CS. More specifically, this main objective of the MCS can be broken down into the following specific objectives:

- OBJ1. To manage security processes and services in an efficiency and quality way.
- OBJ2. To run products, processes and services in CS.
- OBJ3. To lead, coordinate and supervise multidisciplinary CS teams.
- OBJ4. To prepare, direct, coordinate and manage competitive projects in CS.
- OBJ5. To research, develop and innovate in the fields related to CS.
- OBJ6. To apply the acquired knowledge to solve problems in CS environments.
- OBJ7. To know legislations, regulations, and standards around CS.
- OBJ8. To communicate knowledge, reasoning and conclusions to general audience.

Every MCS graduated student must have achieved all of the previous stated objectives, so students will have developed and acquired the necessary skills to assume a series of competencies.

3.2 MCS Competences

The competences that students will acquire throughout the MCS are linked to the MCS objectives. These competences are divided into basic, general and specific ones.

MCS Basic Competences. MCS students will demonstrate that they have achieved the following basic competences:

- BC1. To lead multidisciplinary working groups in international environment.
- BC2. To apply solutions that solve the raised problems.
- BC3. To work efficiently, knowing how to organize and plan personal work.
- BC4. To deal with the information to use, identifying the sources and resources.
- BC5. To issue opinions and reasoned judgments on CS based on knowledge.

MCS General Competences. In addition to the basic competences established in the previous section, students must have achieved the following general skills:

- GC1. To acquire knowledge to be real in the development and/or application of ideas.
- GC2. To apply knowledge and to solve problems in new or unfamiliar environments.
- GC3. To integrate knowledge and to formulate judgments based on information.
- GC4. To clearly communicate their conclusions and the supporting reasons.
- GC5. To gain learning skills that allow them to self-directed or autonomous studying.

Specific Competences. All previous competences are complemented by some other specifically linked to MCS, to be precise, referring to each of the CS aspects. These are the following:

- SC1. To manage and organize the CS of a company by providing tangible benefits.
- SC2. To apply efficiently CS risk assessment.
- SC3. To cope with CS legal, regulatory, and standards frameworks.
- SC4. To understand the principles related to criminal acts.
- SC5. To design decision-making processes according to different intelligence models.
- SC6. To be aware of trends and challenges regarding CS threats and vulnerabilities.
- SC7. To be able to design and apply business continuity and disaster recovery plans.
- SC8. To plan and execute specific protection systems for critical infrastructures.
- SC9. To know the best strategies to manage crisis and situations.
- SC10. To prepare, manage, coordinate, and run CS projects.
- SC11. To know and deploy different physical protection systems solutions.
- SC12. To design and supervise plans for people protection.
- SC13. To know the basic requirements and systems for fire protection.
- SC14. To coordinate the different services for electronic protection.
- SC15. To supervise the processes of occupational risks prevention and its legislation.
- SC16. To organize and prepare evacuation and protection plans.
- SC17. To know the criteria to ensure security for public and private entities.
- SC18. To be aware of the importance of the information and its systems security.
- SC19. To know different access control systems models.
- SC20. To apply the appropriate controls to protect networks and telecommunications.
- SC21. To know the advantages and requirements to apply cryptology solutions.
- SC22. To be aware of the importance of complying with international standards.
- SC23. To know methodologies for the acquisition and development of systems.
- SC24. To plan and supervise applications and communications security.

3.3 MCS Curriculum and Program

The MCS proposal is a 60 credits degree and has a marked globalizing character as evidenced by its objectives, the competences that students must demonstrate, and the breadth of its contents. For these reasons, the syllabus does not contemplate the possibility of different specialties within the global framework of CS.

As shown in Table 1, the MCS splits into four modules. Module I, Module II and Module III have three subjects each, while Module IV entails a master degree's thesis.

Table 1. MCS structure. Subjects overview

Module	Subjects	Credits
I: Strategic and Management Aspects within CS	I.1 – CS Management and Organization	5
	I.2 – CS Risk and Crisis Management	5
	I.3 – Law, Criminology and Crime	4
II: Basic Aspects of Physical Security	II.1 – Electronic and Physical Protection	6
	II.2 – Civil Protection, Fire Fighting and Hazards	5
	II.3 – People, Companies and Goods Protection	6
III: Basic Aspects of Cybersecurity	III.1 – Information Security and Cryptology	6
	III.2 – Networks Security and Access Control	6
	III.3 – Systems Architectures, Developments and Operations	5
IV: Master's Thesis	IV.1 – Master's Thesis	12

The following subsections describes MCS modules and their subjects.

Module I: Strategic and Management Aspects Within CS. This is a 14 credits module made up of the following three subjects:

I.1 – CS Management and Organization. This is a five credits subject whose main characteristics are shown in Table 2.

Table 2. I.1 – CS management and organization. Description

Brief description of the contents	Objectives	Competences
Value and contribution of CS; Corporate needs; Integration of CS in organizations; Organizational structures and their operation; Human resources, materials, and activities in CS; Strategies and Tactics in CS; Local CS vs. Global CS; CS and Defense; International organizations and CS trends; Intelligence cycle and models; Strategies and decisions around CS; CS Dashboards and indicators; Bases of business economics; and Financial asset management	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC5, SC6, SC9, and SC10

I.2 – CS Risk and Crisis Management. This is a five credits subject whose main characteristics are shown in Table 3.

Table 3. I.2 – CS risk and crisis management. Description

Brief description of the contents	Objectives	Competences
CS Organizational principles; Planning; anticipation and psychological CS aspects; Communication management; International CS scenarios; Crisis management techniques and models; CS Trends; CS Organizational and functional structures; Business Continuity Plans; Business continuity management systems; Concept and bases of risk; CS Framework and criteria; CS Contextualization, analysis, and risk management; Making judicious decisions: objectives, risks, and costs; CS Continuous improvement and risk management; CS New challenges: threats and vulnerabilities; and Critical infrastructures	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC6, SC7, SC8, SC9, and SC10

I.3 – Law, Criminology and Crime. This is a four credits subject whose main characteristics are shown in Table 4.

Table 4. I.3 – Law, criminology and crime. Description

Brief description of the contents	Objectives	Competences
The legal conception of security as a public service; Citizen security: security forces and bodies; The State for the operation of public security services; Police collaboration and international legal framework; Personal data privacy; Intellectual property and other intangible assets; The National Security and Cybersecurity Strategies; Criminal phenomenology; Forensic profiling; Digital evidences; Fraud prevention and investigation methods; and Professional deontology	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC4, SC6, SC9, and SC10

Module II: Basic Aspects of Physical Security. This is a 17 credits module made up of the following three subjects:

II.1 – Electronic and Physical Protection. This is a six credits subject whose main characteristics are shown in Table 5.

Table 5. II.1 – Electronic and physical protection. Description

Brief description of the contents	Objectives	Competences
Fundamentals of physical and electronic security; Technical protection measures; External protection; Internal protection; Punctual protection; Specifications; Functions and staging of active protection; Intrusion detection; Closed circuit television; Access control; Other protection systems: communications, patrolling, etc.; Integration and centralization of protection systems; and Security approaches in buildings	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC6, SC9, SC10, SC11, and SC12

II.2 – Civil Protection, Fire Fighting and Hazards. This is a five credits subject whose main characteristics are shown in Table 6.

Table 6. II.2 – Civil protection, fire fighting and hazards. Description

Brief description of the contents	Objectives	Competences
Civil protection; Civil Protection and Emergency Management; Risks in civil protection; Systems of Civil Protection and Emergencies; Fire safety; The risk of fire in buildings; Causes and consequences; The Fire Prevention Regulations; Passive fire protection; Active fire protection; Prevention of occupational hazards; CS against occupational hazards; General and specific risks; Risks related to the working environment; and Prevention and protection against occupational hazards	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC6, SC9, SC10, SC13, and SC15

II.3 – People, Companies and Goods Protection. This is a six credits subject whose main characteristics are shown in Table 7.

Table 7. II.3 – People, companies and goods protection. Description

Brief description of the contents	Objectives	Competences
Protection and regulations; Protection Training; Security at large events; Coordination and command centers; Counter surveillance program; European Protection Network; Dynamic protection at international or large summits; Methodology and Implementation of a CS department; Self-protection plans; Permanent coordination centers in protection; CS plan; Access controls and accreditations; Airspace and CS; Private CS and the Private CS Law; Competences and public authorities; Institutional participation and social recognition; Private CS activities; Companies and detective offices; Private CS personnel; CS services. Private CS measures; Administrative control and sanctioning regime; and Collaboration between public and private CS	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC4, SC6, SC9, SC10, SC14, SC16, and SC17

Module III: Basic Aspects of Cybersecurity. This is a 17 credits module made up of the following three subjects:

III.1 – Information Security and Cryptology. This is a six credits subject whose main characteristics are shown in Table 8.

Table 8. III.1 – Information security and cryptology. Description

Brief description of the contents	Objectives	Competences
Steganography; Mathematical foundations of CS; Symmetric cryptography: stream and block encryption; Random Number Generation (RNG); Key agreement protocols; Asymmetric cryptography: RSA; Elliptic curves; Hash functions; Digital signature schemes; Public key infrastructure: digital certificates; (Post)Quantum cryptography; Side channel and fault induction attacks; and Biometric systems and identification of people	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC6, SC9, SC10, SC20, and SC21

III.2 – Networks Security and Access Control. This is a six credits subject whose main characteristics are shown in Table 9.

Table 9. III.2 – networks security and access control. Description

Brief description of the contents	Objectives	Competences
Confidentiality, Integrity and Availability Requirements; Protocols: PPTP, IPsec, L2TP, SSL/TLS, SSH; Network devices and definition of collision domains; Security protocols in WLAN networks; Security in Bluetooth, NFC and RFID interfaces; Security in WSN: ZigBee (IEEE 802.15.4); Security in VANETs networks; Security in GSM/UMTS/LTE mobile networks; Access control mechanisms through smart cards; Access control methodologies; Authentication mechanisms; Anonymity and privacy: main concepts and challenges; and Tor networks	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC6, SC9, SC10, SC18, and SC19

III.3 – Systems Architectures, Developments and Operations. This is a five credits subject whose main characteristics are shown in Table 10.

Table 10. III.3 – Systems architectures, developments and operations. Description

Brief description of the contents	Objectives	Competences
Products and systems certifications; Common Criteria and Other certifications; Forensic analysis of computer systems; Evidence: obtaining, analysis, custody, and procedures; Forensic analysis tools; Exploitation of software vulnerabilities; Exploitation of web systems; Vulnerability management; Cyber defense systems; Audit and analysis of events; Attack detection systems; Security Information and Event Management Systems; Malicious code: analysis and engineering; and Cyber espionage	OBJ1, OBJ2, OBJ3, OBJ4, OBJ5, OBJ6, and OBJ8	BC1, BC2, BC3, BC4, and BC5; GC1, GC2, GC3, GC4, and GC5; SC1, SC2, SC3, SC4, SC6, SC9, SC10, SC22, SC23, and SC24

Module IV: Master's Thesis. The Master's Thesis (MT) is the culmination of the acquisition of knowledge throughout the MCS. MT is a 12 credits original work that cannot be presented until all the 48 teaching credits of the MCS have been passed, although its subject must begin to be considered by students from the beginning of the MCS to guarantee a choice aligned with their preferences and interests.

The MT pursues the implementation and development of the methodological and theoretical knowledge acquired during the MCS through the preparation and defense

of an individual and original research work, of a theoretical or empirical nature, that collects most of the aspects dealt with in the subjects of the MCS.

The MT would focus on any of the topics proposed by the academic committee of the MCS or any other proposed by the student and accepted. Some potential topics for the MT are the following: CS risk assessment for a company and its impact on business; definition and deployment of CS in an international organization; design of a CS and crisis management model in an organization; or analysis of the regulatory and legal framework in force in terms of CS and its impact on controls.

MCS Schedule and Faculty. Professors and professionals with wide experience in their corresponding MCS's subjects could lead the MCS classes and master classes. All the MCS's subjects would have, at least, one master class in charge of a well-recognized and prestigious professional or researcher, as well as several invited speakers from academic and organizations institutions, both public and private.

Every subject would have a responsible in charge of ensuring the correct development of that subject. In addition, he would safeguard the delivery of all content, the availability of teaching materials, the existence of a unified teaching criterion for other teachers of the same subject, as well as a clear and equitable method of evaluating the subject.

It is important to note that the MCS teaching staff would be composed by professionals with a big experience in different fields and academics (with PhD title). This fact would be strongly conditioned by the special contents that are contemplated in the first two modules. Module III contents are usually part of the study plans of many universities, mainly in Mathematics, Engineering, etc. For Module I and Module II subjects, there could be prestigious specialists with wide professional and teaching experience assigned to each of those subjects. Nevertheless, an academic commission to achieve MCS objectives would coordinate all MSC subjects.

4 Conclusions

Coordination and communication are key elements in order to keep assets protected in an organization. Although CS can be a challenge, it generates an advantage within organization, especially in terms of efficiency and, consequently, sustainability.

Since CS promotes synergies for the security function in organizations by eliminating duplicities and optimizing dedications and efforts around processes, requirements, resources, or budgets, among others. One of the strategic levers for CS deployment in an organization is education, training and the promotion of CS culture, facilitating the acquisition of knowledge and skills.

To date, the authors have not found any university master's degree or similar regulated education. Current university education is focused on cybersecurity or safety as isolated topics instead of a greater approach as CS.

To fill this gap and provide a unifying perspective, this paper shows a master's degree proposal, whose main purpose is the complete training of professionals in CS. On this premise, the MCS intends that all professionals can face any challenge in CS, being able to define, present, and/or develop effective and efficient CS strategies.

As a result, the students who graduated from the MCS will be able to provide a comprehensive approach to the CS risks of an organization. This constitutes a more accurate and solid perception than if risks were assessed separately. A detailed CS assessment provides better risk management strategies for an organization, thanks to wide perspectives of threats, vulnerabilities, and controls perspectives.

Additionally, MCS promotes sustainability through efficiency and rationalization on the general asset protection process, by eliminating functional gaps and promoting cost savings, either by reducing expenses, or by avoiding them. In this sense, redundant functions can be removed and processes can be optimized. This means an improvement in cost control and productivity for the organization.

Finally, MCS collaborates in improving the CS culture inside the organization. This has a direct impact on reducing the number of CS incidents, decreasing their intensity, and increasing the reputation and image of the organization, both internally and externally.

Acknowledgement. This research has been partially supported by the Department of Information and Communication Technologies (TIC) at Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC).

References

1. Data Never Sleeps 8.0: <https://www.domo.com/learn/data-never-sleeps-8>. Accessed 18 May 2021
2. World Economic Forum: The global risks report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Accessed 18 May 2021
3. Kledt, F., Evers, P., Benson, D.: Section II.2 - Organizational Complexity. In: Contemporary Theory and Practice of Organizations. Part I. Understanding the Organization. Ibidem-Verlag, Stuttgart, pp. 95–116 (2016). <https://cup.columbia.edu/book/contemporary-theory-and-practice-of-organizations/9783838267470>
4. Rahman, S.M., Donahue, S.E.: Convergence of corporate and information security. *Int. J. Comput. Sci. Inform. Sec.* 7(1), 63–68 (2010). <https://arxiv.org/abs/1002.1950v1>
5. Cabric, M.: From Corporate Security to Commercial Force: A Business Leader's Guide to Security Economics. Butterworth-Heinemann, Boston (2017). <https://www.sciencedirect.com/book/9780128051498/from-corporate-security-to-commercial-force>
6. Cabric, M.: Corporate Security Management. Challenges, Risks, and Strategies. Butterworth-Heinemann, Boston (2015). <https://doi.org/10.1016/C2014-0-04011-7>
7. Kinslow, J.: Physical and IT security: the case for convergence. *J. Sec. Educ.* 75–91 (2006). https://doi.org/10.1300/j460v02n01_06
8. Jovanovic, M., Burbiel, J.: The evolving concept of security: a critical evaluation across four dimensions. In: Proceedings of the 9th Security Research Conference Future Security, pp. 502–506 (2014). https://www.researchgate.net/publication/278033393_THE_EVOLVING_CONCEPT_OF_SECURITY_A_CRITICAL_EVALUATION_ACROSS_FOUR_DIMENSIONS
9. Purpura, P.P.: Security: An Introduction. CRC Press, Boca Raton (2016). <https://doi.org/10.1201/9781439894569>
10. Halibozek, E.P., Kovacich, G.L.: The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, 2nd edn. Butterworth-Heinemann, Boston (2017). <https://www.sciencedirect.com/book/9780128046043/the-managers-handbook-for-corporate-security/#book-info>

11. Stackpole, B., Oksendahl, E.: Security Strategy: From Requirements to Reality. Auerbach Publications, New York (2010). <https://doi.org/10.1201/EBK1439827338>
12. Masters Programs in Cybersecurity: <https://www.masterstudies.com/Masters-Degree/Cyber-Security/>. Accessed 18 May 2021
13. Masters Programs in Security: <https://www.masterstudies.com/Masters-Degree/Security/>. Accessed 18 May 2021
14. Masters Programs in Safety Management: <https://www.masterstudies.com/Masters-Degree/Safety-Management/>. Accessed 18 May 2021
15. ANECA, Listado de titulaciones: <https://srv.aneca.es/ListadoTitulos/busqueda-titulaciones>. Accessed 7 Jun 2021
16. ISACA's Certified Information Security Manager – CISM. <https://www.isaca.org/credentialing/cism>. Accessed 18 May 2021
17. ISC²'s Certified Information Systems Security Professional – CISSP: <https://www.isc2.org/Certifications/CISSP>. Accessed 18 May 2021
18. Gartner's Top 10 Security Predictions 2016: <https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/>. Accessed 18 May 2021
19. Microsoft Corporation, Accenture LLP: Future of physical security whitepaper-Extending converged digital capabilities across logical & physical environments, 2018. https://www.accenture.com/_acnmedia/PDF-100/Accenture-Future-of-Physical-Security-Whitepaper.pdf