Univerza *v Ljubljani*
Fakulteta *za gradbeništvo*
in geodezijo

VÍTOR FERRONATO DE LIRA

CYBERSECURITY OF COMMON DATA ENVIRONMENTS OF SENSITIVE ASSETS

KIBERNETSKA VARNOST SKUPNIH PODATKOVNIH OKOLJ OBČUTLJIVIH NEPREMIČNIN

BIM A+ European Master in Building Information Modelling

Master thesis No.:

Supervisor:
Prof. Žiga Turk, Ph.D.

Ljubljana, 2020

Co-funded by the Erasmus+ Programme of the European Union

ERRATA

Page	Line	Error	Correction

»This page is intentionally blank«

BIBLIOGRAFSKO – DOKUMENTACIJSKA STRAN IN IZVLEČEK

UDK: **004.056.53:69.01(043.3)**

Avtor: **Vítor Ferronato de Lira**

Mentor: **prof. dr. Žiga Turk**

Somentor:

Naslov: **Kibernetska varnost skupnih podatkovnih okolj občutljivih nepremičnin**

Tip dokumenta: **magistrsko delo**

Obseg in oprema: **85 str., 45 sl., 13 tab., 1 pril.**

Ključne besede: **BIM, kibernetska varnost, digitalna okolja za sodelovanje, občutljive nepremičnine**

Izvleček: Količina digitalnih podatkov, proizvedenih v zadnjem desetletju ali dveh, se je zaradi digitalizacije gradbene industrije bistveno povečala. Digitalizacija je del disruptivnih inovacij, ki ustvarjajo različne priložnosti za sektor, zlasti z uvajanjem metodologije in tehnologije BIM. Zaradi tako radikalnih inovacij se pojavljajo vprašanja kibernetske varnosti, ki lahko ogrožajo informacijsko infrastrukturo z uničujočimi učinki, kot so uničenje datotek, izguba občutljivih podatkov in kraja intelektualne lastnine. Splošni cilj naloge je raziskati vprašanja varnosti, posebej varnosti skupnih podatkovnih okolij (CDE) za občutljive nepremične, konkretno kaznilnice in zapore. Z analitično metodo naloga preiskuje literatura o kibernetski varnosti s poudarki na digitalnih okoljih za načrtovanje zaporov: najprej naloga opravi pregled literature v zvezi z BIM in kibernetsko varnostjo; razišče in opravi kvantitativno zbiranje podatkov v zvezi z zapori in varnostnimi izzivi, ki vključujejo infrastrukturo, ki omogoča pretok informacij v fazi načrtovanja projekta; na koncu opravi analizo ranljivosti CDE in predlaga varnostne ukrepe za zmanjšanje tveganj kibernetske varnosti. Naloga ugotavlja, da so postopki kibernetske varnosti za zaščito skupnega digitalnega okolja še na začetku. Dalje naloga ugotavlja, da so ranljivosti CDE neposredno povezane s kritičnostjo celotne infrastrukture procesa načrtovanja stavb. Zajema človeške vire, fizične in digitalne sisteme. Samo zaščita celotne infrastrukture je način za zagotovitev varnosti CDE. Študij te problematike bi kazalo nadaljevati z izdelanimi vprašalniki, ki bi preverili stanje v praksi in z razvojem "modela varnostne zrelosti", ki bi industriji omogočili preverjanje ustreznosti pristopa k organizaciji kibernetske varnosti.

»This page is intentionally blank«

BIBLIOGRAPHIC– DOCUMENTALISTIC INFORMATION AND ABSTRACT

UDC: **004.056.53:69.01(043.3)**

Author: **Vítor Ferronato de Lira**

Supervisor: **Prof. Žiga Turk, Ph.D.**

Cosupervisor:

Title: **Cybersecurity of common data environments of sensitive assets.**

Document type: **Master thesis**

Scope and tools: **85 p., 45 fig., 13 tab., 1 appx.**

Keywords: **BIM, Cybersecurity, collaborative digital environment, sensitive assets.**

Abstract: Digital data volume produced in the last decade or two has been increasing substantially due to the digitisation of the construction industry. The digitisation process is part of disruptive innovations, which create diverse opportunities for the sector, particularly through the adoption of the BIM methodology and technology. Along with the disruptive innovations, there emerge cybersecurity issues that may compromise an organization infrastructure with devastating effects such as file destruction, sensitive data loss and theft of intellectual property, citing just a few examples. To that effect, this study has the general goal to investigate the cybersecurity issues involving the CDE of sensitive assets, particularly case, penal buildings. Through the analytical method, it shall be investigated the cybersecurity issues involving the collaborative digital environment of penal buildings: at first, it makes a literature review to understand the "state-of-art" regarding BIM and cybersecurity; then it investigates and performes a quantitative data collection relating to penal buildings and the security challenges involving the infrastructure which enables the information flow during the project design phase; at the end, it performs an analysis upon the CDE vulnerabilities, proposing security measures to mitigate cybersecurity risks. This research concludes that the adoption of cybersecurity procedures to protect the collaborative digital environment of a sensitive asset is still at its beginnings. It stresses that the CDE vulnerabilities are directly related to the criticality of the whole infrastructure of the building design process, i.e. it embraces the "Human Sources", the "Physical" and the "Digital" systems. Thus, protecting the whole infrastructure is a way to assure protection of the CDE. In the future the application of the research questionnaires developed for this study is suggested, and the development of a "maturity model" to measure and classify the organization's cybersecurity approach.

»This page is intentionally blank«

ACKNOWLEDGEMENTS

I would like to express my gratitude to my mentor prof. dr. Žiga Turk, by his guidance and principally by sharing with me his knowledge and experience. Also, for providing the necessary information for the development of this research study.

I would also like to extend my gratitude to prof. dr. Tomo Cerovšek, as the Course Coordinator from the University of Ljubljana - Slovenia, by organizing and providing the necessary information about the procedures for the development of this research study.

I would like to extend my sincere thanks to prof. dr. Miguel Azenha, as the Director of the BIM A+ Master Course, by his great effort applied for the development of the master course.

I would like to thanks prof. dr. José Granja, as the Course Coordinator from the University of Minho – Portugal, by his helpful contributions.

I gratefully acknowledge the assistance of all the professors from the three institutions participant of this European Consortium: the University of Minho, University of Ljubljana and Politecnico di Milano, for transmitting me their knowledge and professional experiences.

I would like to recognize the assistance received from Ana Fonseca, Secretary of the BIM A+ Master Course, from the University of Minho.

I would like to recognize the assistance received from Romana Hudin, Head of Office of International and Research Activity, and Iztok Lovišček, both from the University of Ljubljana.

I would also like to extend my deepest gratitude to my family, and principally to my mother Rita Ferronato, that has always been being my emotional and spiritual guide and support.

I would also like to thank my friends from Brazil. Principally to prof. dr. Luciane Cleonice Durante and all the other team members from the Laboratory of Technology and Thermal Comfort (LATECA), from the Federal University of Mato Grosso (UFMT) for sharing their knowledge with me during the last years.

Special thanks to all my friends from the master course, who helped me a lot and became great friends.

I also thank all of those who direct or indirectly helped me.

»This page is intentionally blank«

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

LIST OF ACRONYMS

AEC/FM	Architecture, Engineering and Construction/Facility Management
BDIS	Big Data Intelligence System
BEP	BIM Execution Plan
BIM	Building Information Modelling
BJS	American Bureau of Justice Statistics
CDE	Common Data Environment
CIA	American Central Intelligence Agency
CPS	Cyber-Physical Systems
DDM	Direct Digital Manufacturing
DEPEN	Brazilian National Penitentiary Department
EIR	Exchange Information Requirements
ENISA	European Network and Information Security Agency
EU	European Union
FBI	Federal Bureau of Investigation
FSB	British Finance Stability Board
GAO	The US Government Accountability Office
GDP	Gross Domestic Product
HDI	Human Development Index
ICPR	Institute for Crime & Justice Policy Research
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IT	Information Technology
LAC	Latin America and Caribbean
NSA	American National Security Agency
OSINT	Open Source Intelligence
PCC	First Command of the Capital
RIBA	Royal Institute of British Architects

TAL	Threat Agent Library
UK	United Kingdom
UNDP	United Nations Development Programme
USA	United States of America
WHO	World Health Organization

1 INTRODUCTION

Businesses models have changed their dynamic and the world started being more connected, where traditional businesses models cannot follow innovations, disrupting what once existed and affecting global economic sectors. The AEC/FM industry is considered the most significant world economy branch, is an essential industry. It employs a considerable amount of workforce, taking a substantial role in the GDP in different nations: only the USA government invested $334 billion in 2018 on public infrastructure [1]. Besides, the sector also presents the contribution of 13 per cent of the global GDP [2].

Comparing with other industries that have technologically evolved a lot and exponentially since the past decades, however, this evolution did not happen with the AEC/FM industry on the same proportions. The industry is trying to "change the scale" on its favour, through the implementation of new methodologies and technologies. As mentioned by Mantha & Soto [3] "(…) the construction industry is making a shift towards digitization and automation due to rapidly growing information and communication technologies such as 3D printing, blockchain, and robotics." Principally in a moment when it is widely spoken about smart buildings, embodied energy and climate change.

Furthermore, both the private and public sectors have been played the role of implementing new methodologies and technologies. Principally the public sector, realizing the benefits of the technological wave. According to Bartlett et al. [2], "some governments are taking action to spur innovation on public projects." The methodologies are training professionals to develop high-specialized information management skills, and technology has helped them to work collaboratively and interconnected.

Working collaboratively and interconnected means that professionals are storing, sharing and managing information within collaborative digital environments and not necessary at the same physical environment anymore. In this sense of interconnectivity, Waugh [4] said that, by the end of 2018, there would "be more than eight billion internet of things (IoT) devices connected worldwide, according to analysts Gartner – from electricity meters to smart fridges".

Besides, the reality showed up by the advent of working collaboratively and interconnected is also engaged by Tapscott and Williams [5] when they say that "'In an age where mass collaboration can reshape an industry overnight, the old hierarchical ways of organizing work and innovation do not afford the level of agility, creativity, and connectivity that companies require to remain competitive in today's environment.'" The agility and connectivity mentioned are possible through the implementation of the BIM methodology and technology.

1.1 Problematic

BIM methodology and technology adoption has enabled to produce data on a giant scale and in a way the world has never seen before. Data is an "atom" in a whole web, which aggregation is responsible for

providing value on information. In this sense, data is an asset for any organization, because it detains information about: its production practices, capital investment, personnel's information, intellectual property and others.

Although BIM technology provides a collaborative environment and interconnectivity among professionals, there are some side effects and hazards that must be taken into account. People need to be vigilant about where they store their data and to whom they are sharing it with [4]. Some malicious insiders and outsiders are just waiting for the best opportunity to cause large-scale damages, causing unprecedented problems for the organization for uncountable reasons.

The inconsistent adoption of BIM technologies may cause unexpected vulnerabilities to Cyber-dependent crimes. According to the IOCTA report [6] "Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)". The report also adds that "The European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 identified cybercrime as one of the 10 priorities in the fight against organised and serious international crime".

The IOCTA report [6] also informs that "As more and more companies outsource areas of their business, such as moving more infrastructure to third-party cloud services, we expect to see a growth in supply chain attacks, and the evolution of such attacks to become increasingly complex. Interdependency between organisations leads to the necessity of having a higher level of cybersecurity across the spectrum to ensure the minimisation of successful cybercrime attacks." The IOCTA report also informs that cybercrimes can "(…) seriously impact the physical, financial and psychological safety, security and stability of our society and require a coherent and coordinated response by law enforcement".

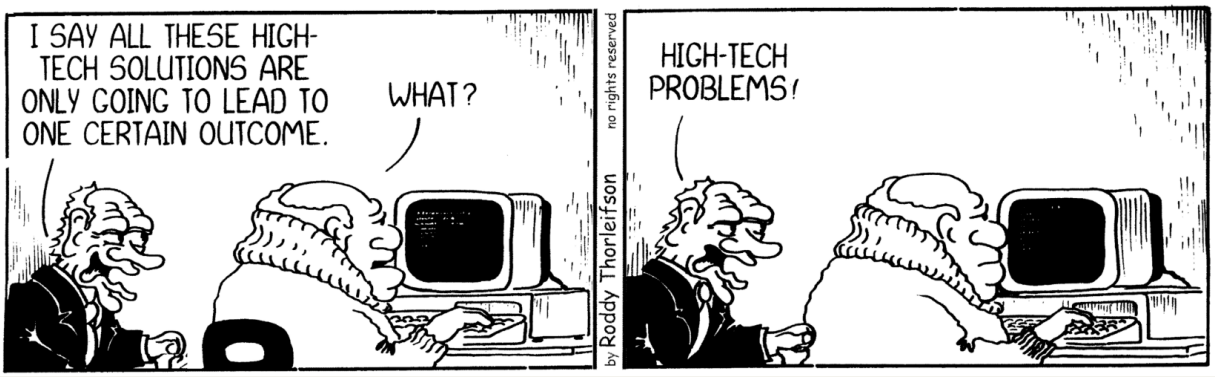

Figure 1: technological solutions – technological problems. Cartoon by Roddy Thorleifson. Source: mooselakecartoons.com

1.2 Justification

Besides, the AEC/FM industry is also vulnerable to cybersecurity issues. Despite the new horizon of possibilities provided by a collaborative digital environment, it is getting hard to manage information

without risks. According to Hammi & Bouras [7], "the problematic comes from how to secure the sensitive data and how to manage the pertinent documents between inter-disciplinary teams." The authors call the attention for the need to "the need to address cyber security awareness and implementation on collaboration systems and coordination processes."

Hammi & Bouras [7] also mention that "Such a complicated collaboration environment when using BIM involved varied teams from the AEC sector is creating automatically security issues, the fact that industrials do not have the same levels of security understanding and standards. Moreover, the change of the interfacing people and the growth of the supply chain during the project lifecycle make the protection of the information uncontrollable and more complex."

Mantha & Soto [3], on their study about the cybersecurity challenges on the Civil Construction industry, report some security incidents involving the sector, mentioning about the "stolen floorplan files of the Australian intelligence headquarters in 2013 (Motley & Mas, 2017)", the economic risks faced "during the collection of deposits from applicants in the name of Komatsu, a well-known Japanese construction machinery manufacturer", and that "A lot of construction employees' tax details and social security numbers of a US-based construction company, Turner, were compromised due to data sharing through unsecured channels posing business-related risks (Watson, 2018)."

Nevertheless, Mantha & Soto [3] say the reality of the investments on cybersecurity system and practices for the AEC/FM industry is not enough, "making this industry susceptible and particularly attractive to hackers (Watson, 2018)."

Furthermore, according to Coburn et al. (2019) cited by Soto et al. [8], the 2019 Cyber Risk Outlook "identifies key AECO-relevant trends such as Increasing Exposure to Digital Attack and Disruption, Increasing Propensity for Cyber-Induced Business Interruption, Attacks on Digital Supply Chains, Growing Potential for Cyber-Physical Loss Events, Cyber Attacks Becoming Increasingly Political, and Changing Motivations of Threat Actors."

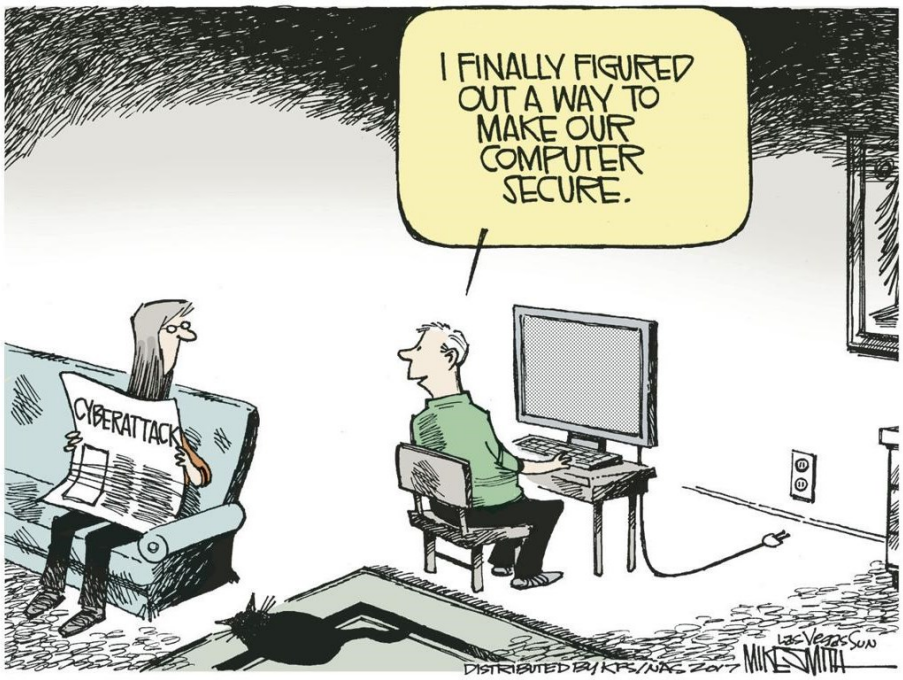

Figure 2: internet "security". Cartoon by Mike Smith. Source: https://lasvegassun.com

1.3 Objective

Despite the imminent cybersecurity risks addressed to the AEC/FM sector, little has been said about the cybersecurity risks involving sensitive assets, principally the ones affecting the collaborative digital environment, used during the project design phase. Therefore, this study has the general goal to investigate the cybersecurity issues involving the CDE of sensitive assets, particularly case, penal buildings.

1.4 Methodology

Through the analytical method, it shall be investigated the cybersecurity issues involving the collaborative digital environment of penal buildings. At the first moment, it shall be made a literature review to understand the "state-of-art" of some topics regarding BIM and Cybersecurity.

On the sequence, it shall investigate information upon penal buildings, the necessary infrastructure to enable the information flow during the project design phase, and cybersecurity issues. Besides, the quantitative data collection method is also used to present consistent information. By the end, it shall be performed an analysis of all the investigated information.

Finally, it shall be presented the conclusions upon the performed analysis with recommendations for future works.

1.5 Thesis' structure

Six chapters structure the thesis. The first chapter is the introductory part. It presents a general overview of the AEC/FM industry, BIM and Cybersecurity issues involving the sector; besides, it is shown the objective and the methodology used for the development of the study. The other chapters provide an investigation upon the topics of interest; a further analysis of the problematic; and a conclusion of what shall be discussed here. A better understanding and brief description of each chapter are given subsequently.

LITERATURE REVIEW corresponds to the second chapter. This chapter shows the "state-of-art" of the following topics: sensitive assets, BIM, collaborative digital environment and Cybersecurity, which are the basis for the development of this study.

PENAL BUILDINGS corresponds to the third chapter. This chapter briefly presents the concepts and architectural models of penal buildings throughout the centuries. Besides, it is also given an overview of the world penitentiary population and the social and economic impacts caused by the penal system.

SECURITY CHALLENGES corresponds to the fourth chapter. It starts presenting an overview upon cybercrimes, malicious agents, cyber threats and as well as examples related to them. Later on, the chapter presents existing building design practices and its supporting infrastructure.

CYBERSECURITY MEASURES corresponds to the fifth chapter. An investigation is performed within this chapter upon existing proposed cybersecurity measures that shall be applied to avoid/mitigate cyber threats and cyber-attacks. Thus, the first subsection gives an overview of cybersecurity measures; the second subsection informs about cyber-resilience, and the third and last subsection tells about propositions to cybersecurity.

ANALYSIS corresponds to the sixth chapter. This chapter presents a review from the investigation performed in the previous chapters, analyzing the correspondences between the investigated topics of interest. First, it is presented some vulnerabilities of the CDE. Next, it is introduced a Cybersecurity Protocol, to avoid/mitigate the enumerated cybersecurity risks; then, it presents an assessment on cybersecurity. Besides, this chapter is complemented by APPENDIX A.

At the CONCLUSIONS, it is done some considerations over the process. Moreover, it is presented some recommendations for future works on the cybersecurity field.

APPENDIX A presents the research questionnaires developed to assess the cybersecurity engagement of a supplier and its supply chain involved within the development of a project design phase for penal buildings.

2 LITERATURE REVIEW

This chapter represents the thesis' theoretical part, in which the context and essential concepts shall be presented, discussed and elaborated; i.e. the "state-of-art" of the ideas are introduced. Besides, in this chapter, it shall be explored what other researchers have found about cybersecurity issues and whether those findings are connected or not with the common data environments of sensitive assets.

2.1 Sensitive Assets

Starting by a semantical analysis, the complete understanding of "sensitive asset" is preceded by the individual meaning of each word. According to the online Cambridge Dictionary, there are some definitions of the word "sensitive", relating more to objects than people:

- easily influenced, changed, or damaged by a particular thing;
- needing to be treated with care or secrecy;
- easily influenced or affected by something; and
- used to describe a subject, situation, etc. that needs to be dealt with carefully or kept secret.

From the definitions given above, it can be inferred that "sensitive" is a "thing" that can be easily influenced, changed or damaged.

On the other hand, the definition of "asset" by the online Oxford Learner's Dictionary informs that "asset" means:

- a person or thing that is valuable or useful to somebody/something; and
- a thing of value, especially property, that a person or company owns, which can be used or sold to pay debts.

The PAS 1192-5 [9] and the ISO 19650-1 [10] informs the same definition for an asset: "item, thing or entity that has potential or actual value to an organization".

Considering the definitions above around the term "asset", it can be understood that an asset is something owned by an organization, such as money, property and other, that has is useful and or valuable.

Therefore, considering the scarce definitions for "sensitive" and "asset", the term "sensitive asset" here is understood as: an entity/property that has potential or actual value owned by an organization.

Once presented information about the sensitive assets, the following subsection comments about BIM.

2.2 Building Information Modelling

Eastman et al. (2011) say that BIM "has orchestrated a paradigm shift in the way that information is managed, exchanged and transformed, to stimulating greater collaboration between stakeholders who interact within a Common Data Environment (CDE) throughout the building/infrastructure asset's whole lifecycle" [11].

Arayici et al. [12] inform that BIM "is a methodology to integrate digital descriptions of all the building objects and their relationships to others in a precise manner, so that stakeholders can query, simulate and estimate activities and their effects on the building process as a lifecycle entity", that, like Eastman et al., have a similar approach upon the collaboration topic on BIM, mentioning "integration" on their study.

The PAS 1192-2 [13] states that BIM is a "process of designing, constructing or operating a building or infrastructure asset using electronic object-oriented information."

The PAS 1192-5 [9] has the same approach as the PAS 1192-2 [13], informing that BIM is a "discrete set of electronic object-oriented information used for design, construction and operation of a built asset" [9].

For the ISO 19650-1 [10], BIM is a "use of a shared digital representation of a built asset to facilitate design, construction and operation processes to form a reliable basis for decisions." Here is possible to see that the BIM description is similar to the ones presented at the Project Execution Planning Guide [14], regarding the sharing of information. Furthermore, the digital representation approach is similar to the one presented by Arayici et al. [12], the PAS 1192-2 [13] and the PAS 1192-5 [9].

Castaing et al. [15] inform that "Building information modelling (BIM) is a digital information management approach being adopted by the construction industry to improve productivity and quality in building and infrastructure projects, reduce financial losses during construction, and provide a basis for developing future services."

According to the Little Book of BIM [16], BIM is "a collaborative way of working underpinned by digital technologies, which allow for more efficient methods of designing, delivering and maintaining physical built assets throughout their entire lifecycle." The collaboration activity enabled by the BIM methodology described at the Little Book of BIM [16] is also similar to the one presented by Eastman et. al.

Abdelhameed & Saputra [17], say that BIM "is an approach and a process in which the design model potentially includes various building information of different components and spaces, in order for the users to visualise, manage, analyse and/or design in a better way."

Therefore, it is concluded that BIM is a methodology for the process of designing, constructing or operating a building/infrastructure during its entire life cycle in which the digital representation of information is prepared, within a collaborative digital environment. An illustration of the BIM methodology can be seen in Figure 3:

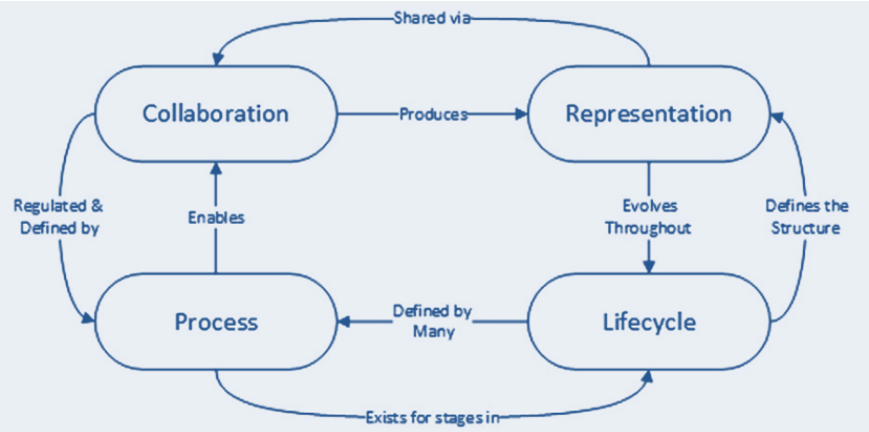

Figure 3: "BIM in a Nutshell" 4 key elements of the BIM concept. Source: Bradley et al. [18]**.**

With the purpose to accomplish the design task of a well-developed federated model within a collaborative digital environment, it is necessary to understand it. This subject is explored in the next subsection.

2.3 Collaborative Digital Environment

According to Lou & Alshawi [19], collaborative environments "(…) present a platform whereby various construction professionals involved in a construction project could come together and to address project needs. This environment offers a standard platform for all parties involved to communicate, exchange data and information, data storage, archiving and much more."

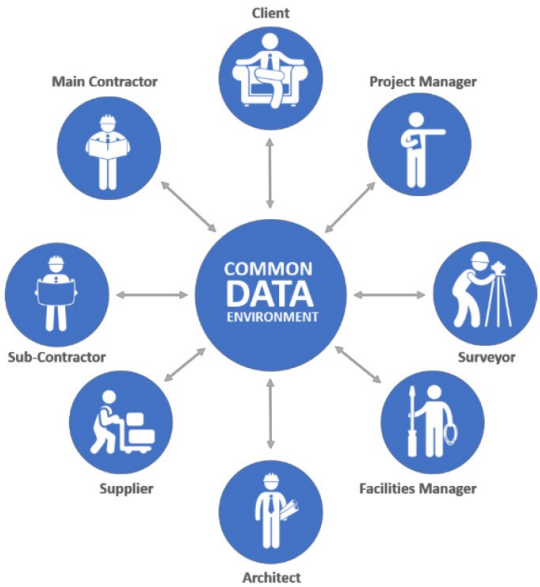

Figure 4: CDE concept. Source: adapted from Scottish Future Trust [20]**.**

The PAS 1192-2 [13] states that a collaborative digital environment, calling it as CDE, is "used to collect, manage and disseminate all relevant approved project documents for multi-disciplinary teams in a managed process."

Boyes [21] informs that the CDE "(…) provides a single repository for information for any given project, which is used to collect, manage and disseminate all relevant approved project documents for multi-disciplinary teams as part of a managed process."

The PAS 1192-5 [9], states that the CDE is a "single source of information for any given project or built asset, used to collect, manage and disseminate all relevant approved files, documents and data for multidisciplinary teams in a managed process." The standard also informs that it is not recommended that sensitive information is contained within a CDE "(…) unless that CDE is held within a secure environment."

The ISO 19650-1 [10] defines CDE as an "agreed source of information for any given project or asset, for collecting, managing and disseminating each information container through a managed process". The ISO 19650-1 [10] presents the following CDE organization, seen in Figure 5:

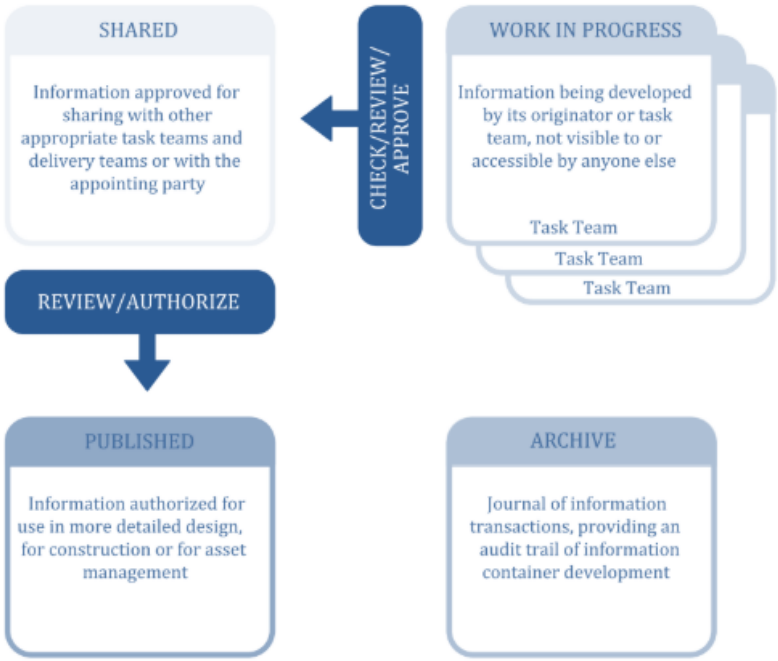

Figure 5: CDE concept. Source: adapted from ISO 19650-1 [10].

Therefore, from the information given above, it can be understood that a CDE is a digital platform/repository for information for any given project whereby diverse professionals involved in a construction project collect, manage and disseminate all relevant approved files, documents and data for multidisciplinary teams in a controlled process.

Given the presentation around the CDE, the cybersecurity subject is then, presented.

2.4 Cybersecurity

The word "cybersecurity" is a joint of two other words: "cyber" and "security", where the first is a newer concept when compared with the second one, probably due to the technological development of the last decades. Using the same principle of checking the semantical meaning of the words, here developed the understanding over the cybersecurity theme.

According to the online Cambridge Dictionary, the word "cyber" means:

- involving, using, or relating to computers, especially the internet;

Besides, the online Oxford Learner's Dictionary says that cyber is:

- connected with electronic communication networks, especially the internet;

From the definitions above, it is inferred that "cyber" is something connected with computers and electronic communication networks, especially the internet.

On the other hand, according to the online Cambridge Dictionary, the word "security" means:

- protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries;
- the fact that something is not likely to fail or be lost;
- the protection of information against being stolen or used wrongly or illegally.

Moreover, the online Oxford Learner's Dictionary informs that "security" is/are:

- the activities involved in protecting a country, building or person against attack, danger, etc.;
- protection against something bad that might happen in the future.

According to the definitions presented by the dictionaries, "security" may be defined as the protection of a person, building, organisation and other, against threats or attacks.

The concept of security, according to what states the PAS 1192-5 (2015), "(…) operates on a number of levels ranging from national security issues (e.g. protection against terrorism and detecting hostile acts by nation states), to tackling organized crime, and to preserving the value, longevity and ongoing use of an enterprise's assets, whether tangible (e.g. a building or physical stock), or intangible (e.g. preventing the loss or disclosure of intellectual property and nationally or commercially sensitive information)"; in this study, security operates in the second statement, connected with the idea of "(…) preserving the value, longevity and ongoing use of an enterprise's assets."

As said by Boyes [22], on his study upon cybersecurity addressed to intelligent buildings, he says that "An internationally agreed definition of Cybersecurity is 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets'".

On another work, Boyes [21] also mentions that "Cyber security is about more than technology; it encompasses people, process and governance issues, and their inter-relationships. These non-technical elements are management issues and are as important in Cybersecurity as the deployment of appropriate technical solutions."

As stated by Craigen et al. [23], "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de *jure* from *de facto* property rights."

Barrett [24] informs that cybersecurity is "The process of protecting information by preventing, detecting, and responding to attacks". He also adds that "Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line (…) can drive up costs and affect revenue (…) harm an organization's ability to innovate and to gain and maintain customers (…) be an important and amplifying component of an organization's overall risk management".

Mantha & Soto [3] say that "Cybersecurity can be defined as tools, policies, and practices to protect the data (stored and transmitted) and assets such as computers, infrastructure, and personnel (ITU, 2019). The exposure to cyberattacks in the construction industry is amplified by the number of stakeholder and the long supply chains, mostly consisting of small businesses with limited resources devoted to information technology (IT)."

Therefore, "cybersecurity" is understood as "the protection of information from an electronic communication network against danger/threats such as crime or attacks".

Besides, from the investigation above, it is realized that only in the PAS 1192-5 [9], within Boyes' [21] [22] and in Mantha & Soto [3] studies is recognised the most significant approaches to the theme explored in this research. However, it is still absent specific information regarding cybersecurity addressed to common data environments of sensitive assets. Therefore, this study shall explore more about the topic.

After this literature review, the next chapters shall present an investigation upon the existing literature and data collection. This strategy is a basis to develop this study, with the purpose to clarify and sediment the study approach. Starting by the "PENAL BUILDINGS" chapter, it presents the fragility of the penitentiary system, how it may influence the policies of a nation and the social and economic impacts.

3 PENAL BUILDINGS

Penal buildings are part of the criminal and correctional systems of any nation, representing a sensitive asset due to its social and economic impacts. As human society has evolved its perspectives upon the criminal and correctional systems, the penal buildings architectural models have also changed during the centuries. Moreover, the project design practices and strategies were also developed and improved, enabled by the technological revolution the humankind has been experiencing.

By "technological revolution" it is understood the advancements into the AEC/FM industry, through the implementation of the BIM methodology and its supportive technology, as an example. Also, the CDE is the centre core of this supportive technology, once it enables the collection, management and dissemination of "each information container through a managed process" [10]. Hence, the CDE is understood as part of the project design infrastructure and as an essential tool for the project design management. Besides, special attention must be given to the CDE security, considering the significant losses that may occur caused by a cybercriminal attack.

Therefore, this chapter shall present information about the penal building's architectural concept and model; the world incarcerated population; and the social and economic impacts of the criminal and correctional systems.

3.1 Architectural Concept and Model

Moral and ethical behaviours have always been a discussion-centre regarding the human society internal organization. However, behaviours against the established moral and ethical patterns are punished based upon criminal codes that have been evolving during the centuries as the human perception changes. Intentionally, the creation of the penal system and its buildings aims to separate criminal conducts from life in society.

The study of Michel Foucault[1] [25] is the principle to understand the penal buildings' concept. The author says that prison architecture permits "an internal, articulated and detailed control (…); in more general terms, an architecture that would operate to transform individuals: to act on those it shelters, to provide a hold on their conduct, to carry the effects of power right to them, to make it possible to know them, to alter them."

Foucault also mentions the early adoption of the "panopticism" at the architectural building concept, saying that "The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being

[1] Michel Foucault (1926–1984) was »a French historian and philosopher, associated with the structuralist and post-structuralist movements«. Source: https://plato.stanford.edu/entries/foucault/

seen" [25]. He also adds that "the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."

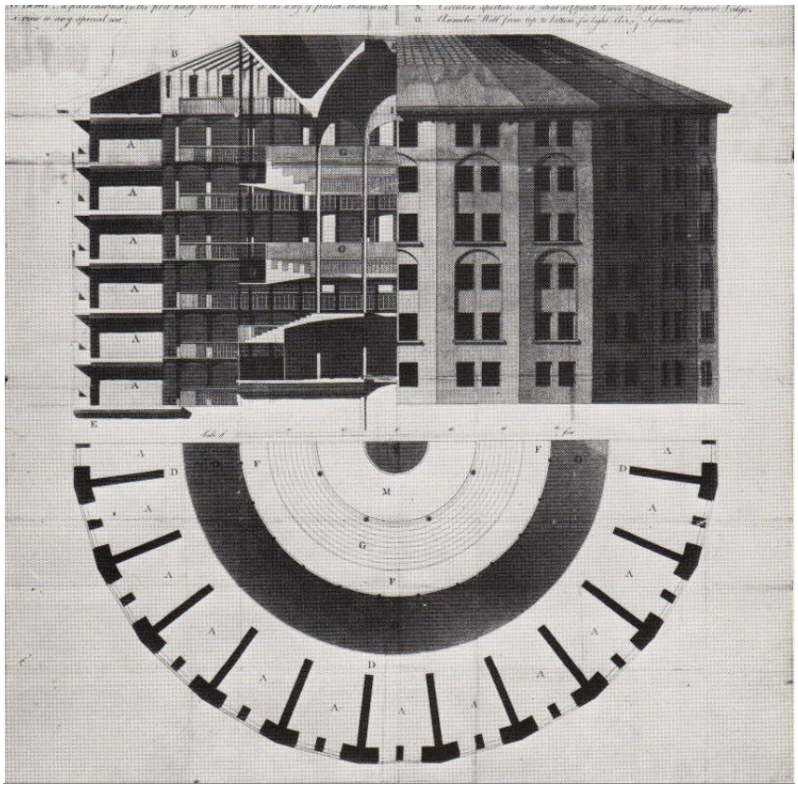

Figure 6: 1791 design for the Panopticon by Jeremy Bentham, Samuel Bentham and the architect Willey Reveley. Source: Steadman [26]**.**

Foucault mentions that Baltard[2] called the prison institution as "'complete and austere institutions' (Baltard, 1829)." The authors say that "In several respects, the prison must be an exhaustive disciplinary apparatus: it must assume responsibility for all aspects of the individual, his physical training, his aptitude to work, his everyday conduct, his moral attitude, his state of mind; the prison, much more than the school, the workshop or the army, which always involved a certain specialization, is '*omni*-disciplinary'" [25].

Eight years after the publication of Foucault's book, Henley brings the idea of a new prison typology. The author says that "The 21st Century Model Prison seeks to define a new prison typology organised to achieve freedom of activity and inhabitation for the prisoner. The prisoner is enabled to engage in a range of activities inside and outside the building, supported by a circulation and management system that brings the human expertise to the prisoner environment" [27].

Henley says that the new design "inverts the logic of Bentham's Panopticon 'inspection house'" [27], adding that "The model evolved to enable learning to be integrated in to all aspects of prison life and to

[2] Louis Pierre Baltard, also known as Louis-Pierre Baltard (1764-1846). He was a French architect and printmaker. Source: The British Museum: https://www.britishmuseum.org/collection/term/BIOG18285

be integrated into every space, the objective being to enable prisoners to resettle into society with a significantly reduced incidence of recidivism" [27].

Further, the author presents the new model opposite characteristics regarding the panopticism idea: "In the Panopticon and radial prison (e.g. HMP Pentonville, 1842) we find a building type designed to separate and "warehouse" people (…). By contrast, the new model is founded on the principle of learning and training, where the prisoner lives in a semi-autonomous unit, or house, adjacent to a "roundabout" of efficient circulation, which feeds directly to each of the spatial components of the prison. Within the house the prisoner is a member of an accountable group, living close to external space, defined and controlled by a chequerboard array of buildings and external courtyard gardens" [27].

Muir and Loader [28] also bring information about the designing of prisons, saying that: "The power of prison design to affect people both within and outside prison walls was well understood by those who built prisons in the 18th and 19th centuries; (…). Prison exteriors were deliberately crafted to instil fear and communicate a message of deterrence. The interiors were designed to change the prisoner in certain ways, especially through a focus on solitary personal reflection in individual cells."

From above, it is understood the early concept of incarceration and penalty and the inhuman prison design characteristic, is also confirmed through Yvonne Jewkes'[3] words: »(...) it is certainly the case that those earliest prisons, built for a 'separate system' of total solitude, are among the bleakest and most inhuman, for that was the intention when they were designed and built« [29].

From the conception of penalisation and the best approach for prison design, it is further analysed the actual activities addressed to the penitentiary system. Victoria Knight[4] [29] interviews Steven Van De Steene[5] about the digitisation project of prison in Belgium (PrisonCloud). According to Victoria's, Steven »(...) draws our attention to important features of digitization identifying the successes and challenges for making this valuable transition within the context of the prison.«

Along with the article, it is possible to infer that the technological revolution has been applied to the penitentiary system. The PrisonCloud »is a flexible IT platform designed for the secure distribution of content and services to inmates. It provides inmate services at any time, in any allowed location within the controlled prison facility. It allows the inmate to be responsible for his own life in prison while

[3] Yvonne Jewkes »is Research Professor in Criminology at the University of Brighton and is Principle Investigator on an ESRC-funded study of prison architecture, design and technology« [29].
[4] Victoria Knight »is a senior research fellow for the Community and Criminal Justice De Montfort University« [29].
[5] Steven Van De Steene »is an Enterprise Architect and Technology for Corrections Expert. He works as a consultant in the area of innovation and technology strategy for prisons and probation services and is the coordinator of the Technology Solutions Group for the International Prisons and Corrections Association (ICPA)« [29].

offering a platform for both entertainment and work«, according to the E-BO Enterprises[6], the company responsible for developing the IT platform.

Considering the prison digitisation idea, it is inferred that content from the PAS 1192-5 [9] could be applicable at this PrisonCloud project, once it brings »Specification for security-minded building information modelling, digital built environments and smart asset management«.

After briefly informed about the prison's concept and architectural models, the next subsection presents information upon the global penitentiary population, followed by the social and economic impacts to keep functioning the penal system.

3.2 Incarcerated Population

As life becomes improving, many countries are closing or retrofitting buildings that once housed detention activities. The Netherlands and Portugal[7] are examples of it. As reported by Weller [30], "In 2013, 19 prisons in the Netherlands closed because the country didn't have enough criminals to fill them." However, there are still many countries facing considerable problems in criminal activities. Thus, this item briefly presents some data about the worldwide criminal reality, once it is not the intention to a more profound discussion about it.

According to the World Prison Brief[8], the ranking of the ten countries hosting the worldwide most significant incarcerate population is presented in Figure 7:

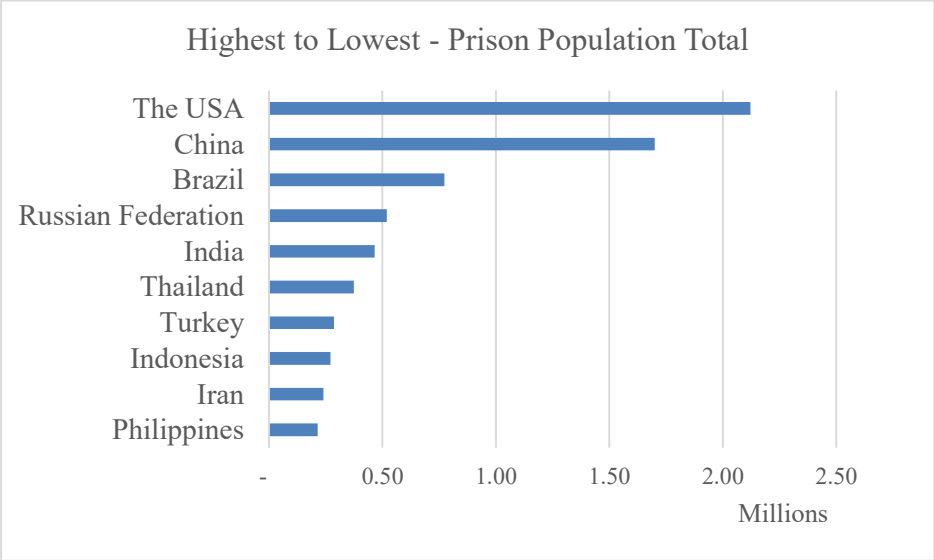

Figure 7: world prison population total. Source: World Prison Brief website, access on the 5th of April of 2020. Chart art: the author.

[6] E-BO Enterprises: https://www.ebo-enterprises.com/prisoncloud
[7] Portuguese Centre of Photography: a previous jail and court of appeal building. Location: Porto city, Portugal.
[8] Organization hosted by the ICPR, at Birkbeck, University of London.

The chart above shows that the USA is the leading country of the biggest incarcerate population (2.121.600,00) ranking in the world, followed by China (1.700.000,00), Brazil (773.151,00), the Russian Federation (518.391,00) and India (466.084,00).

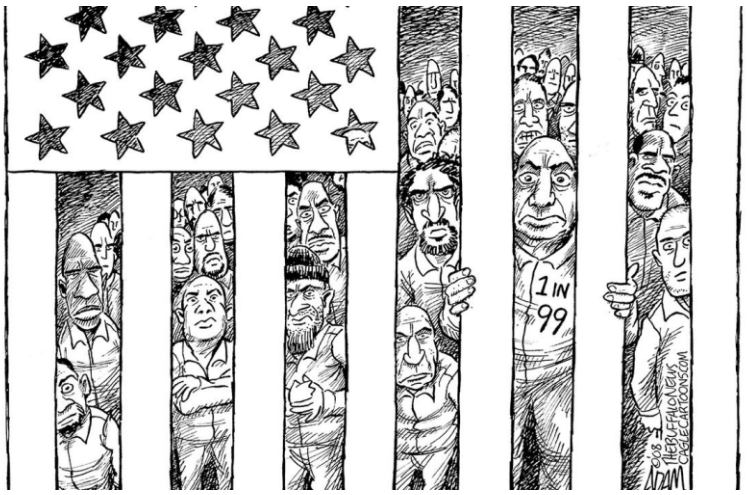

Figure 8: illustration of the US Prison System. Cartoon by Adam Zyglis/Cagle Cartoons. Source: https://www.duluthnewstribune.com

Furthermore, searching for the USA criminal cases, it was found out information about the Alcatraz prison (Figure 9) at the FBI [9] official website page. The FBI webpage informs that the Alcatraz (also known as "The Rock") prison "surrounded by the cold, rough waters" is located in an island at the middle of San Francisco Bay and had held incarcerated people since the American Civil War (1861-1865). In 1934, as informed by the article, the prison was re-fortified, becoming the "world's most secure prison". From 1934 to 1963, when the prison was closed, 36 men tried 14 separate escapes.

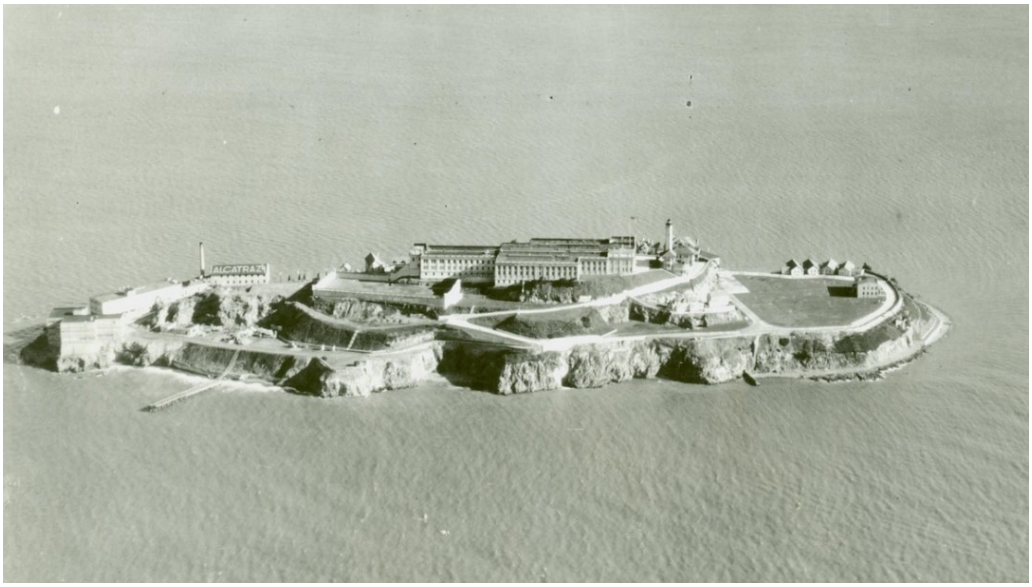

Figure 9: aerial view of Alcatraz Island, January 1932. Source: FBI.

[9] The domestic intelligence and security service of the USA: https://www.fbi.gov/history/famous-cases

The prison inspired the famous “Escape from Alcatraz” film (based on in a homonymous book), a production from the American film studio “Paramount Pictures Corporation”.

The human creativity has inspired another prison-related entertainment production. This is the case of the fictional TV movie named “Prison Break”, produced by the 20th Century Fox Television. The plot tells a story about Michael Schofield (Wentworth Miller), a structural engineer who “resolves to bust his sibling [Lincoln Burrows, interpreted by Dominic Purcell] out of the notorious Fox River State Penitentiary[10].” To help to release his brother from the jail, Michael tattoos on his body (Figure 10) the penitentiary floor plans.

Figure 10: Michael Schofield's tattoos. Source: adapted from https://www.tattoodo.com/a/prison-breaks-michael-scofield-is-back-and-his-tattoos-might-be-too-7167

Another fictional production about prisons is the “Escape Plan” movie, starred by Sylvester Stallone, Arnold Schwarzenegger. Performed by Ray Breslin (Sylvester Stallone) a structural-security authority and his fellow inmate Emil Rottmayer (Arnold Schwarzenegger), the story is based on an escape attempt from “the most protected and fortified prison ever built[11]. « The following synopses gives information aobut the movie: “Ray Breslin is the world’s foremost authority on structural security. After analyzing every high security prison and learning a vast array of survival skills so he can design escape-proof

[10] https://www.netflix.com/pt-en/title/70140425
[11] https://www.rottentomatoes.com/m/escape_plan

prisons, his skills are put to the test. He's framed and incarcerated in a master prison he designed himself. He needs to escape and find the person who put him behind bars[12]."

Figure 11: Escape Plan (2013) poster. Source: adapted from https://www.imdb.com/title/tt1211956/mediaviewer/rm1689494528

Leaving the fictional world, Brazil also calls one's attention by its the high number of incarcerated people, coincidently from the American Continent. Brazil currently counts on 1.435 prison units[13] spread over its 26 states and the Federal District and, from this total, five prison units are of maximum security.

Brazilian security reality has been facing several problems for decades. Moreover, the criminal factions that operate within the country are partly responsible for that. There are gang leaders that command criminal acts from inside the prisons. Furthermore, time by time, there are coordinated illegal operations that try to release them.

Alessi [31] informs on his article how the gangs challenge the country's penal system: "Three PCC[14] leaders were murdered between June and July 2015 in prisons on the orders of the FDN". Later on, according to Stargardte [32], it still possible to realize the presence of the same criminal organizations

[12] https://www.thehollywoodnews.com/2013/09/20/take-fist-first-clip-stallone-schwarzeneggers-escape-plan/
[13] According to the DEPEN database - 2019. DEPEN is the executive agency that "monitors and controls the application of the Penal Execution Law and the guidelines of the National Penitentiary Policy, issued mainly by the National Council for Criminal and Penitentiary Policy." Source: http://depen.gov.br/DEPEN/
[14] PCC is a Brazilian gang.

in the country: “Reuters visited the federal jail in Brasilia where (…) several other PCC leaders are being held”.

3.3 Social and Economic Impacts

In terms of social impact, on his article on the psychological effects of incarceration, Haney [33] says that »The adaptation to imprisonment is almost always difficult and, at times, creates habits of thinking and acting that can be dysfunctional in periods of post-prison adjustment. (…) At the very least, prison is painful, and incarcerated persons often suffer long-term consequences from having been subjected to pain, deprivation, and extremely atypical patterns and norms of living and interacting with others. «

Haney also mentions terms upon incarceration and their differences, explaining that: “The term ‘institutionalization’ is used to describe the process by which inmates are shaped and transformed by the institutional environments in which they live. Sometimes called ‘prisonization’ when it occurs in correctional settings, it is the shorthand expression for the negative psychological effects of imprisonment. (…) In general terms, the process of prisonization involves the incorporation of the norms of prison life into one’s habits of thinking, feeling, and acting” [33].

On further explanation, the author presents some examples of psychological adaptations caused by the process of institutionalization, as follows:

a) Dependence on institutional structure and contingencies;
b) Hypervigilance, interpersonal distrust and suspicion;
c) Emotional over-control, alienation, and psychological distancing;
d) Social withdrawal and isolation;
e) Incorporation of exploitative norms of prison culture;
f) Diminished sense of self-worth and personal value; and
g) Post-traumatic stress reactions to the pains of imprisonment.

Haney informs about the presence of psychological implications due to the transition from prison to home, explaining that “The psychological consequences of incarceration may represent significant impediments to post-prison adjustment. They may interfere with the transition from prison to home, impede an ex-convict’s successful re-integration into a social network and employment setting, and may compromise an incarcerated parent’s ability to resume his or her role with family and children” [33].

Moreover, it is presented an analysis of the economic impact of the incarceration activity. Making a cross-data analysis between – the world’s most significant incarcerate population and the world’s biggest economies – it is possible to make some inferences. Some of the world’s fourth-biggest economies also leads the incarcerate population ranking: the USA, China, Brazil and India, from the highest to the lowest numbers. Besides, from the four countries, two of them are located in the American

Continent: the USA (North America) and Brazil (South America). Such information is confirmed in Figure 12.

These are the world's biggest economies

Based on data from the International Monetary Fund, 2018

	Country	Value (in trillions)
1	United States	20.4
2	China	14
3	Japan	5.1
4	Germany	4.2
5	United Kingdom	2.94
6	France	2.93
7	India	2.85
8	Italy	2.18
9	Brazil	2.14
10	Canada	1.8

Source: IMF

Figure 12: world's biggest economies 2018 report. Source: World Economic Forum.

Obtained the data above, it was wondered the worldwide estimated money expenditure with the criminal system. Thus, Farrell and Clark (Farrell & Clark, 2004) informed that it was estimated for 1997 "(…) that the world spent $360 billion on criminal justice in 1997. Of this total, 62 percent ($222.5 billion) was spent on public policing, 3 percent ($11.2 billion) on prosecutions, 18 percent ($63.5 billion) on courts, and 17 percent ($62.5 billion) on prisons."

Furthermore, the authors also cite, through the words of Newman and Howard (1999), that "Previous research has identified a strong relationship between a country's economic welfare, measured as GDP, and its expenditure on criminal justice" [34]. They add that "Not surprisingly, on average, richer countries spend more per capita on criminal justice than poor countries. In this study, the relationship between GDP and spending on criminal justice is examined using data for seventy countries." As an example illustrating the previous statement, the United States of America[15] was the country with the highest value of prison expenditure per capita in the world with an amount of approximately US$ 90,00, presented in Figure 13:

[15] According to Stephan (Stephan, 2004), on his study for the American BJS, in 2001 the sum of the values of all the USA states prison costs was about US$29.5 billion, being US$104,00 each year per USA resident. Besides, the annual operating costs per inmate was US$22,650. Moreover, Stephan (2004) also mentions in his study that, for the fiscal year of 2001, the American State expenditure with the prison construction costs was about US$860,954.

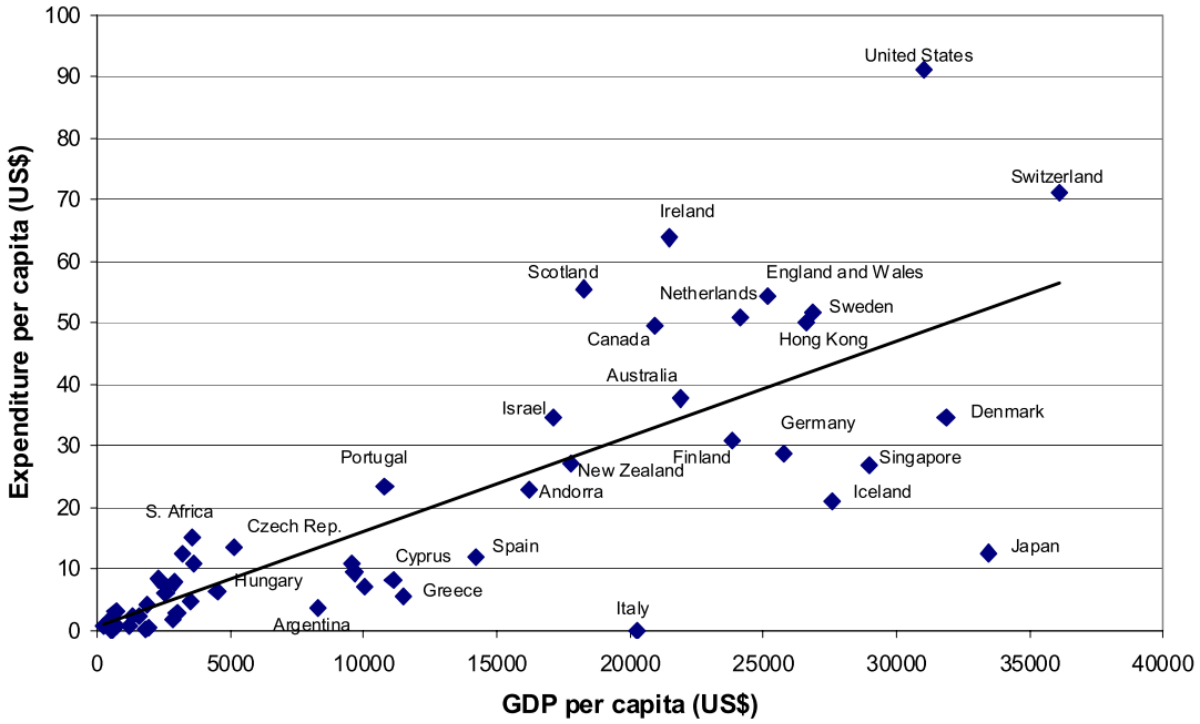

Figure 13: World Prison Expenditure and GDP - 1997. Source: Farrell & Clark [34]**.**

Besides, the GDP percentage addressed to crime-related costs from LAC countries are higher than those considered as developed ones [35]. This comparison is presented in Figure 14:

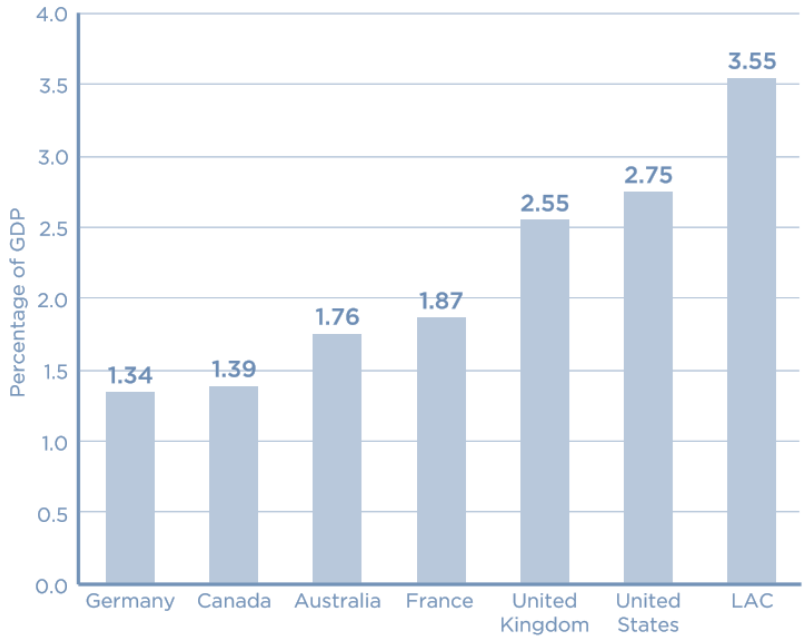

Figure 14: mean crime-related costs, international comparison. Source: adapted from The Inter-American Development Bank [35]**.**

On a recent study, the EU countries spent about € 25.000,00 (Eurostat) with prisons, keeping it almost constantly during the years. This information is presented in Figure 15:

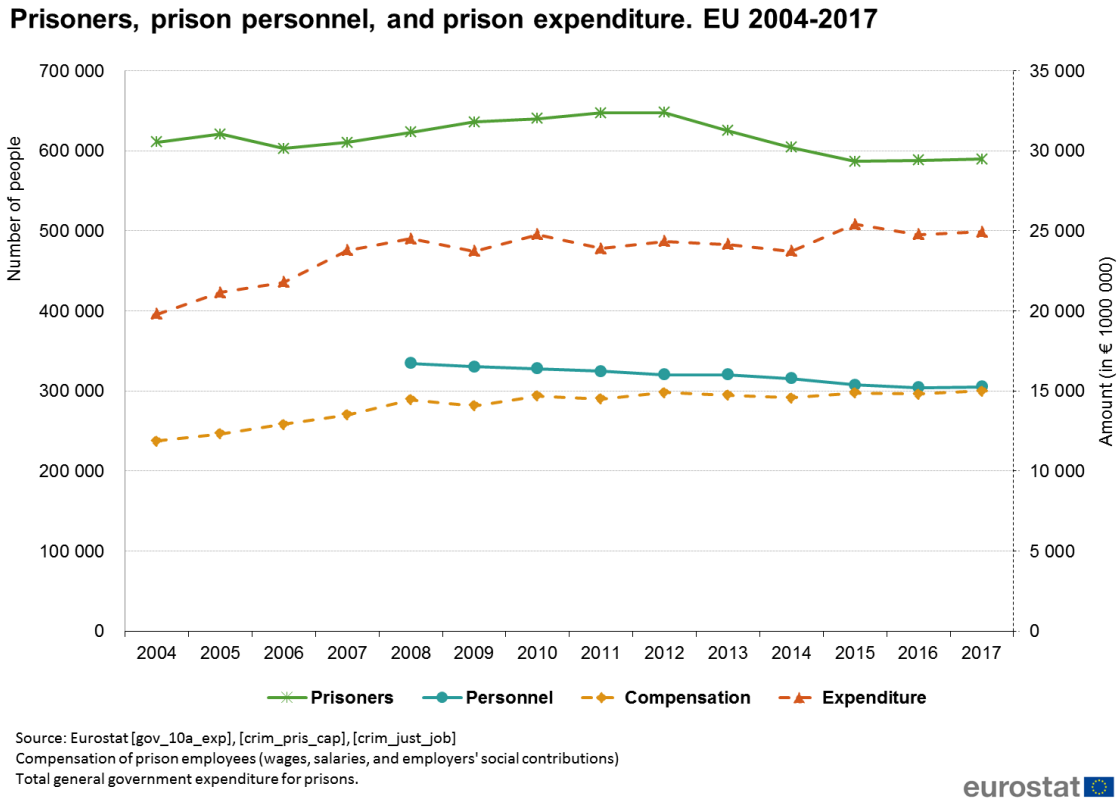

Figure 15: prisoners, prison personnel, and prison expenditure. Source: Eurostat.

After the cross-data analysis exercise, where it was realized the correspondence between the "world's biggest incarcerate population" and the "world's tenth biggest economies", the question about the BIM implementation status in those four countries remains. Professionals around the globe are still struggling to implement the BIM methodology and technology on their workspaces, remaining some reluctance on its adoption.

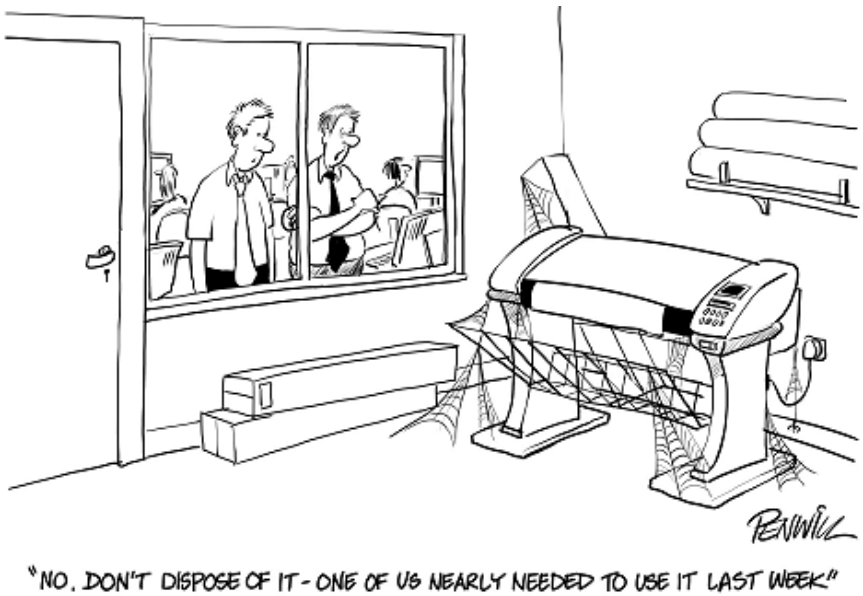

Figure 16: BIM implementation. Cartoon by Roger Penwill. Source: https://www.cadalyst.com

In this sense, Silva et al. Silva et al. (2016) present information about the global BIM implementation status, illustrated in Figure 17:

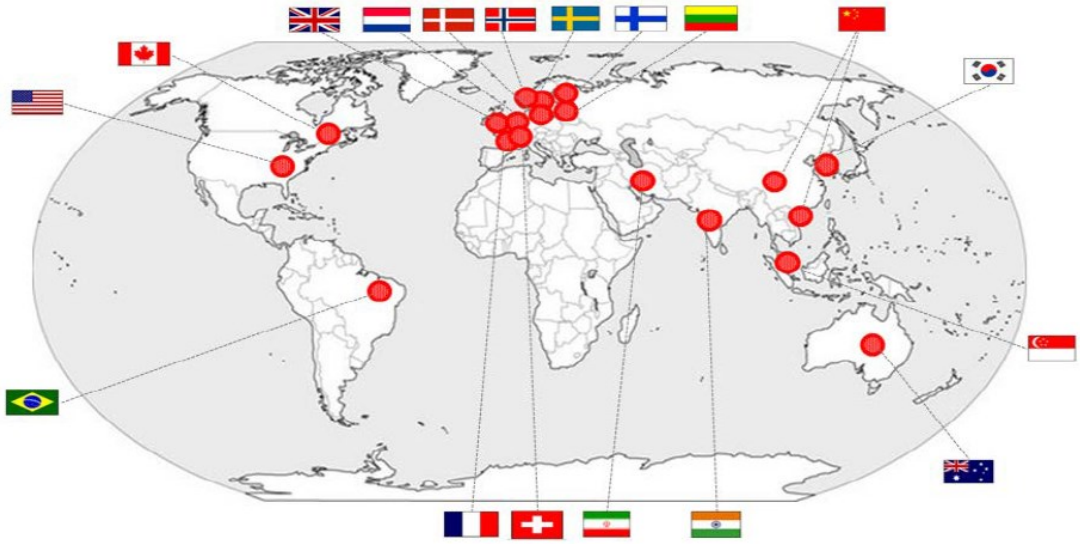

Figure 17: a global perspective of BIM implementation throughout the world. Source: Silva et al. [36].

From this research study, it is presented the BIM implementation status from The USA, China, Brazil and India, respectively, in Table 1:

Table 1: the countries' adaptation to BIM in the construction industry. Information source: Silva et al. [36]**.**

Country	Description
The USA	The General Services Administration requires mandatory BIM submission for government projects since 2008. They are experts in using BIM and are leading BIM practice.
China	BIM has been included as part of the National 12th Five Year Plan (2011-2015) for Mainland China and is formulating a BIM framework. It was created a partnership between Academy of Building Research Technology and Autodesk for BIM models. The Hong Kong Institute of Building Information Modelling (HKIBIM) was established in 2009 and the Hong Kong Housing Authority set a target of full BIM implementation in 2014/2015.
Brazil	Began to be implemented in 2006 in some private initiatives. In 2010 ABNT/134 EEC Special Commission to Study the implementation was created. In 2011 BIM was widespread to public initiatives.
India	In India BIM is also known as VDC: Virtual Design and Construction. It has many qualified, trained and experienced BIM professionals who are implementing this technology in Indian construction projects and also assisting teams in the USA, Australia, UK, Middle East, Singapore and North Africa to design and deliver construction projects using BIM.

Focusing at the Brazilian BIM reality, the latest governmental update about it is a Decree-Law n. 10.306 from the 2nd of April of 2020 that establishes "the use of Building Information Modeling at the direct or indirect execution of engineering works and services carried out by agencies and entities of the federal public administration"[37].

The Decree-Law also establishes the BIM first implementation phase will gradually start in 2021. The Decree-Law also mentions that BIM "shall be used at the development of architectural and engineering design projects, as to new building constructions, building enlargements or rehabilitation (…)" [37]. Hence, considering that the Brazilian National Penitentiary Department is an agency of the federal public administration, it must adapt itself to attend the law requirements.

Therefore, some addition is made to the sensitive asset definition made before: it is an entity/property [**penal buildings**] that has potential or actual value [**social and economic**] owned by an organization [**public sector – governments**].

After the approach to prison systems, the next chapter shall present investigations upon the security challenges involving existing building design practices.

4 SECURITY CHALLENGES

This chapter presents the security challenges involving the CDE infrastructure of penal buildings, during its project design phase. First, it shall be given information about cybercrimes, malicious agents and cyber threats, showing some examples of them. Next, it informs about the existing building design practices, proceeded by its critical infrastructure.

According to Mavroeidis and Bromander, the global crime survey from the PricewaterhouseCoopers[16] (PwC) organization reports that "there are organizations that had suffered cybercrime losses over $5 million, and of these nearly a third reported losses in excess of $100 million" [38].

Besides, it was found out on a Global Threat Intelligence Report [39], issued in 2019, that the Finance and Technology industries led the ranking of the globally most attacked industries' sectors, followed by the Business and Professional Services, Education, Government and others, as presented in Figure 18:

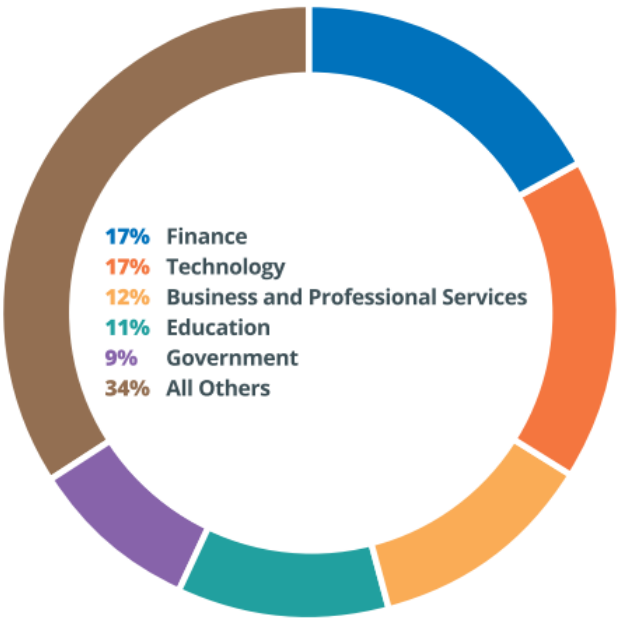

Figure 18: globally most attacked sectors. Source: NTT Global Threat Intelligence Report [39].

Through data presented in Figure 19, it is possible to check that the USA is the prominent global attack source followed by China, Japan, France and The Netherlands. Besides, making a relationship with the information previously presented, it is interesting to realize that the USA and China are amongst not only the global attack sources but also leading the world's economy and incarcerated population.

[16] PwC is »the brand under which the member firms of PricewaterhouseCoopers International Limited (PwCIL) operate and provide professional services. Together, these firms form the PwC network.« Source: https://www.pwc.com/gx/en/about/corporate-governance/network-structure.html

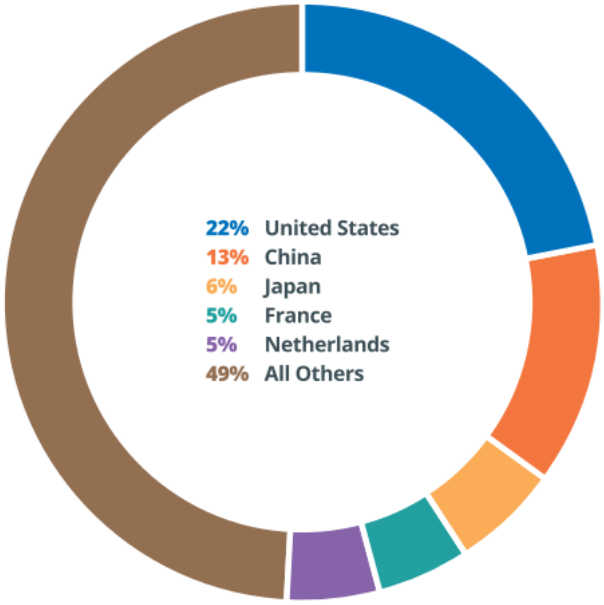

Figure 19: global attack sources. Source: NTT Global Threat Intelligence Report [39].

The Global Threat Intelligence Report also brings the "Global Key Findings" about the cyber-attack matters:

- Finance remained the most attacked sector in 2018, as it has been in six of the previous seven years. It was joined by Technology as a top targeted sector this year.
- 35 percent of all attacks originated from IP addresses within the United States and China.
- Application-specific and web-application attacks accounted for over 32 percent of all hostile traffic, making them the top category of hostile activity.
- 73 percent of all hostile activity falls into four categories: web attacks, reconnaissance, service-specific attacks, and brute-force attacks.

Furthermore, the actions regarding cybercriminal activities may increase due to the current Covid-19 pandemic situation due to the recently necessary work adaptations. The companies and the autonomous professionals needed to change their work methodologies and spaces, depending on more the using of internet services, being more vulnerable to cyber-attacks.

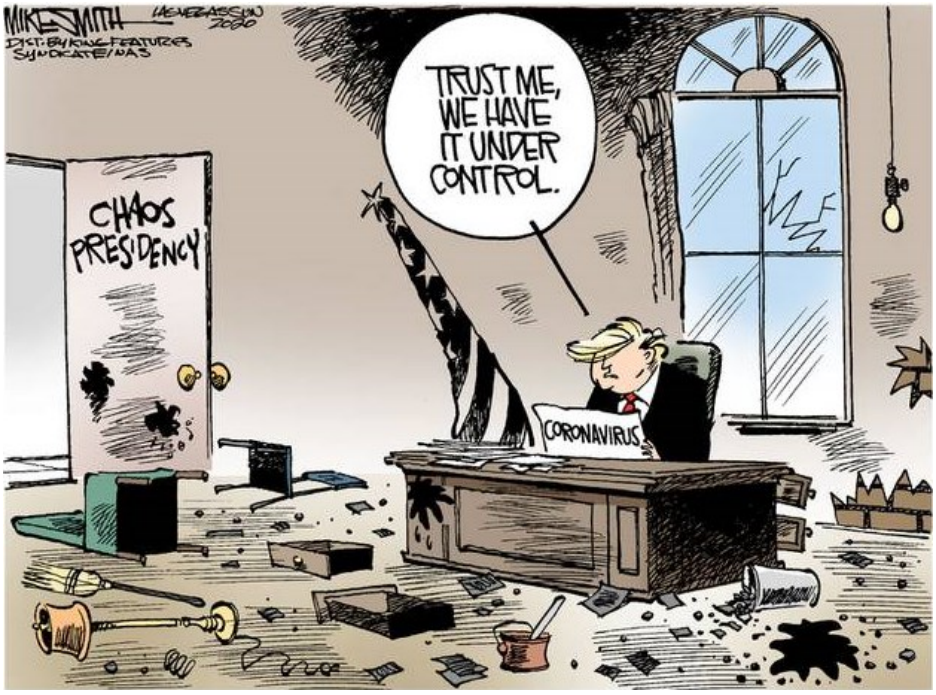

Figure 20: coronavirus pandemic. Cartoon by Mike Smith. Source: https://lasvegassun.com

Moreover, the cybercriminal activities are reported by Joseph Marks and Tonya Riley [40], when they say that: "The massive volume of cybercriminal activity reflects the overwhelming scope of the pandemic, which has upended every aspect of daily life across the world — from how people seek medical information to how they work, socialize and shop for groceries. The mass uncertainty allows criminals to prey on broad swaths of the global population".

Marks and Riley [40], on the same article, report the words of Stephanie Carruthers, a team leader who "focused on studying phishing at IBM's hacking research division." Ms Carruthers says that "'Spammers and scam artists have never had an opportunity like this before'. (…) 'Covid-19 is the first event of its kind since the birth of the Internet. This global pandemic impacts so many different aspects of our lives including physical and financial safety, across geographies for an unpredictable time frame' (…). 'And that's 'a perfect lure' for online criminals'" [40].

Furthermore, according to the authors, the digital security consulting group "Interisle" conclude on its report that "'The pandemic has led to an explosion of cybercrime, preying upon a population desperate for safety and reassurance'". Also, Marks and Riley say that "The number of emails that used phony information about the virus to trick people into infecting their phones and computers has increased by 14,000 percent in just two weeks", according to the IBM's X-Force research division report.

4.1 Malicious Agents

This subsection informs about the malicious/threat agents and the known stages for a cyber-attack. Boyes [41], in his study about the resilience of technology in the built environment, says that threat agents may be considered those who "cause or contribute to a cyber security incident".

Figure 21: malicious agents. Cartoon by Randy Glasbergen. Source: www.glasbergen.com

Boyes [41], has also identified potential threat agents, presented in Table 2:

Table 2: potential threat agents. Source: adapted from Boyes [41]**.**

Threat agents	Description
Malicious outsiders	"This is a person or persons unconnected with the building owner, the building occupier or supporting contractors; in essence, a person who does not have privileged access to the building or its systems. A malicious outsider could be a hacker, a cyber criminal, activist, terrorist or state-supported attacker – in all cases the intent is to cause harm or disruption. The attack may be targeted at the intelligent building and/or its occupants or be indiscriminate, for example malware or viruses."
Malicious insiders	"This is a person (or persons) connected with the building owner, the building occupier or supporting contractors; in essence a person who has some level of authorised or privileged access to the building or its systems and puts that privileged access to a use not intended or allowed."
Non-malicious insiders	"This is a person (or persons) connected with the building owner, the building occupier or supporting contractors, who through error, omission, ignorance or negligence causes a cyber security incident."

Boyes [41] mentions that malicious threat agents may belong to one of the following groups: sole activists, activist groups, competitors, organised crime, terrorist, proxy terror threat agent with nation-state support and nation-states.

Complementary, the Cyber Security Consortium report [21], mentions the following threat agents:

- External threat agents: are malicious outsiders who are unconnected with the building or structure and the professions involved in its design, delivery or operation;
- Internal threat agents: are insiders, i.e. individuals connected with the building or structure and the professionals involved in its design, delivery or operation.

As an example of external threat agents, there is the Julian Assange case. In an article published by "The Guardian" journal, Swaine (2019) informs that the USA government charged Mr Assange about "violating the Espionage Act by publishing classified information through WikiLeaks". The author also mentions that Mr Assange "was previously charged with working to hack a Pentagon computer system (…)".

In contrast with the external threat agents, there are the internal threat ones, and here is presented the Edward Snowden case. Mr Snowden is a former technical assistant for the CIA, who was accused by the USA government of handing over material from the NSA - one of the world's most secretive organisations – according to Greenwald et al. Greenwald et al. (2013). The authors report one of the phrases delivered by Mr Snowden about the fact: "I'm willing to sacrifice all of that because I can't in good conscience allow the USA government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building."

Later on, Wilshusen [44], Director in GAO's Information Technology and Cybersecurity team, stated on his study for the United States Government Accountability Office, the threat agents and their acts' description, informed in Figure 22:

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers/hacktivists	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to potentially have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his February 2015 testimony, the Director of National Intelligence stated that, among state actors, China, and Russia have highly sophisticated cyber programs, while Iran and North Korea have lesser technical capabilities but possibly more disruptive intent.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Figure 22: common cyber adversaries. Source: Wilshusen [44]**.**

Given the information about threat agents, Table 3 presents three different approaches over the topic:

Table 3: threat agents characterization. Source: the author.

Boyes (2013)	Boyes (2014)	Wilshusen et al. (2015)
Malicious insiders	Internal threat agents	Insiders
Malicious outsiders	External threat agents	Hackers/hacktivists, terrorists, criminals

Nevertheless, better than knowing threat agents, it is necessary to understand how to identify them. In this sense, the Intel Information Technology company created a document named TAL [17] [38], which provides »a consistent, up-to-date reference describing the human agents that pose threats to IT systems and other information assets« [45].

[17] Threat Agent Library Helps Identify Information Security Risks. Source: Intel Information Technology.

4.2 Cyber Threats

Given the information about malicious agents, this subsection shall present an approach to cyber threats. Starting by definition, according to the PAS 1192-5 [9], the word "threat" means a "potential cause of an incident which may result in harm to a system or organization."

The UK National Cyber Security Centre document informs that "An attack, particularly if it is carried out by a persistent adversary, may consist of repeated stages" [46]. Besides, it also informs that the attacker is effectively probing the system defences "for weaknesses that, if exploitable, will take them closer to their ultimate goal." The document advises that, if the mentioned stages (Figure 23) are understood, the organization/company/individual can better defend itself.

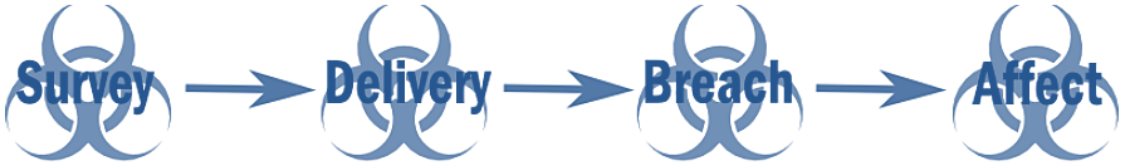

Figure 23: stages in a cyber attack. Source: adapted from the UK National Cyber Security Centre [46]**.**

Furthermore, the document presents the description of each mentioned stages, which can be seen in Table 4:

Table 4: the four stages in a cyber attack. Source: adapted from the UK National Cyber Security Centre [46]**.**

Stage	Description of the Stages
Survey	investigating and analysing available information about the target in order to identify potential vulnerabilities.
Delivery	getting to the point in a system where a vulnerability can be exploited.
Breach	exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.
Affect	carrying out activities within a system that achieve the attacker's goal.

Cichonski et al. [47] on their »Computer Security Incident Handling Guide« for the National Institute of Standards and Technology from the USA Department of Commerce, present information about attack vectors, seen in Table 5:

Table 5: attack vectors. Source: adapted from Cichonski et al. [47]**.**

Attack Vectors	Description
External/Removable Media	An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
Email	An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.

The "systems failures" are also a cybersecurity threat present in the Cyber Security Consortium report [21]. The author mentions that a system failure corresponds to the "failure of storage devices resulting in corrupt or irrecoverable files, or non-availability of critical systems used to store, process or manage BIM data through poor maintenance or a lack of resilience in supporting IT infrastructure." [21]. Besides, more recently, there were again some facts about systems failures[18].

The PAS 1192-5 [9] enumerates some security issues, as follows:

- Hostile reconnaissance;
- Malicious acts;
- Loss or disclosure of intellectual property;
- Loss or disclosure of commercially sensitive information;
- Release of personally identifiable information; and
- Aggregation of data.

In addition to his studies, Wilshusen [44] also shows information about some types of exploits, presented in Figure 24:

[18] In more recent news, the WHO (2020) informed that it "has seen a dramatic increase in the number of cyber attacks directed at its staff (…)". The institution also adds that "some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response." However, the organization is taking preventive measures in order to avoid new cyberattacks, "WHO is now migrating affected systems to a more secure authentication system."

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service/distributed denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Phishing/spear phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Spear phishing is a phishing exploit that is targeted to a specific individual or group.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Figure 24: types of cyber exploits. Source: Wilshusen [44].

Manogaran et al. [5], on their study about big data security intelligence system, addressed to the healthcare industry, relates cybersecurity issues to components of IoT, seen in Table 6:

Table 6: various security requirements and solutions in components of IoT. Source: adapted from Manogaran et al. [5]**.**

Components in the IoT	Vulnerabilities	Types of threats and attacks
Physical objects in IoT	• Physical layer devices have limited Communication, calculation and storage resources • Physical objects are distributed in various regions. Hence, unauthorized user can accesses the devices and performs damages and illegal actions such as reprogram the device, extract security keys and information.	• DoS/DDoS attacks • Physical attacks • Integrating WSNs • Integrating RFID • Unauthorized access control and data access
Communication technologies in IoT	• IoT is a dynamic network infrastructure • Power issues • Network issues • Selection of security technique and its challenges	• Wireless WAN communications • Wireless LAN/PAN communications • Secure IoT communication protocols in constrained resources environment • Secure transmitted data

Applications of IoT	• Data coverage • Cloud computing • Security issues in web application • Secure communication	• DoS • XSS attack • CSRF attack • SQL Injection • Data protection • Data access • PHRs Attacks • Malicious user attacks • Sharing data in different environments • Real-time information processing • Sharing the same sensed data by several applications • Available

In line with the hostile reconnaissance subject presented by the PAS 1192-5 [9], Pärn & Edwards [11], on their study named »Cyber threats confronting the digital built environment«, bring the following information, seen in Figure 25:

	Reconnaissance Technique	Definition
	Scanning — Ping sweep; Port scan; Network Mapping	Network scanning is integral to stealthy information gathering from a computer system. Prior knowledge of the operating system (OS) is combined with the use of one of a plethora of readily available tools, in order to identify and map out potential vulnerabilities on a target network
	Fingerprinting (OS)	Device fingerprinting endeavors to break the privacy of URL developers by revealing user actions and anonymity. It utilizes the information collected from a remote computing device for the purpose of uniquely identifying the device (Formby *et al*., 2016). Fingerprinting can be used to identify the OS used on the target system
	Footprinting	Footprinting is a process of obtaining as much information about the target to be hacked as possible by drawing down open source information from the internet. Footprinting is the most convenient way of gathering information about a computer system and/or parties such belong to
	Sniffing	Sniffing has been likened to wiretapping and can be used to obtain sensitive information that is being transferred over a network, such as: FTP passwords; e-mail traffic; web traffic; telnet passwords; router configurations; chat sessions; and DNS traffic. "Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) sniffing" activites pose an imminent threat to cyber-physical connected devices in buildings, factories and large industrial plants
	Social Engineering	Social engineering is an attack vector that relies upon tricking people into breaking security procedures. Consequently, these are used to exploit an individual's weaknesses, typically employees and other individuals who are familiar with the system. When successfully implemented, hackers can help obtain information about the targeted system

Figure 25: common reconnaissance techniques. Source: adapted from Pärn & Edwards [11]**.**

The authors inform that "Common threats incurred via IT and ICS include: theft of intellectual property; massive disruption to existing operations; and destruction, degradation or disablement of physical assets

and operational ability (Szyliowicz, 2013). The European Union Agency for Network and Information Security outlines multiple common sources of nefarious attacks in its malware taxonomy, including: viruses; worms; trojans; botnets; spywares; scarewares; roguewares; adwares; and greywares (Marinos, 2016)."

On his Global Threat Intelligence Report, Nakata [39] enumerates some web-based attacks, seen in Table 7:

Table 7: web-based attacks. Source: adapted from Nakata [39]**.**

Type of action	Description
Blackmail	(1) a situation in which threats are made to harm a person or organization if they do not do something such as give someone money (online Cambridge Dictionary). (2) the act of putting pressure on a person or a group to do something they do not want to do, for example by making threats or by making them feel guilty (online Oxford Learner's Dictionaries).
Domain Name System (DNS) *Hijacking*	(1) the act of taking control of or using something that does not belong to you for your own advantage (online Cambridge Dictionary). (2) the act of using or taking control of something (online Oxford Learner's Dictionaries).
Dumped Databases	(1) an act of moving information [databases, in this case] from a computer's memory to another place or device (online Cambridge Dictionary). (2) to copy information and move it somewhere to store it (online Oxford Learner's Dictionaries).
Extortion	the crime of making somebody give you something by threatening them (online Oxford Learner's Dictionaries).
Hacktivism	the activity of getting into computer systems without permission in order to achieve political aims (online Cambridge Dictionary).
Identity Theft	the crime of using someone's personal information in order to pretend to be them and to get money or goods in their name (online Cambridge Dictionary).
Input Capture	the information that you put into a computer (online Cambridge Dictionary).
Leaked Credentials	(1) to allow secret information [credentials, in this case] to become generally known (online Cambridge Dictionary). (2) to give secret information to the public (online Oxford Learner's Dictionaries).
Reputation Damage	the opinion that people have about what somebody/something is like, based on what has happened in the past (online Oxford Learner's Dictionaries).
Sell for *Profit*	money that is earned in trade or business after paying the costs of producing and selling goods and services (online Cambridge Dictionary).
Stolen *Credentials*	(1) something such as a document that proves who someone is, what organization they represent, or what their qualifications are (online Cambridge Dictionary). (2) documents such as letters that prove that you are who you claim to be, and can therefore be trusted (online Oxford Learner's Dictionaries).

Trade for Services	the activity of buying and selling or of exchanging goods or services between people or countries (online Oxford Learner's Dictionaries).

There is also the contribution of the IOCTA [6] report over cyberattacks, presented in Table 8:

Table 8: cyber attacks. Source: adapted from IOCTA [6]**.**

Type of attack	Description
Data *Compromise*	to risk having a harmful effect on something [data, in this case]. To lower or weaken standards (online Oxford Learner's Dictionaries).
Data *Stealing*	(1) to take something without the permission of its owner (online Cambridge Dictionary). (2) to take something from a person, shop, etc. without permission and without intending to return it or pay for it (online Oxford Learner's Dictionaries).
Mobile Malware	threats (…) designed to work on mobile platforms (Europol website).
Ransomware	software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money (online Cambridge Dictionary).
Sabotage	(1) the act of intentionally trying to stop someone from achieving something or to stop something from developing (online Cambridge Dictionary). (2) the act of doing deliberate damage to equipment, transport, machines, etc. to prevent an enemy from using them, or to protest about something (online Oxford Learner's Dictionaries).
Website Defacement	the act of damaging the appearance of something [website, in this case], especially by drawing or writing on it (online Oxford Learner's Dictionaries).

As the study developed by the Intel Information Technology company to identify malicious agents, Mavroeidis & Bromander [38] made their contribution to providing a tool which can help with the identification of potential attacks. The authors have established a Cyber Threat Intelligence Model – CTI. The model is a way »to represent what types of information are needed for advanced threat intelligence and potential attack attribution« [38]. The authors also say that “damage infrastructure” is one example of an actor’s goal.

Furthermore, compromising an infrastructure means a significant loss of any type of organization, principally if the infrastructure is operating within a cyber-based network. It was recently identified that “Threats from cyber-crime have arisen partially because of the increased adoption rate of networked devices but also as a result of industry’s operational dependency upon IT systems” [11].

The attacks on cyber-physical infrastructures are also informed on the IOCTA report [6], which says that: “The fourth cyber threat highlighted by European cybercrime investigators was attacks that disrupt or subvert the internal functions of one or more critical infrastructures.”

Besides, Wegner et al. [5] mention that: "The increasing reliance on Computer Aided Manufacturing (CAM) is opening new attack vectors, such as attacks on the initial CAD drawings or its derivatives. Designs can be influenced in a variety of ways (…) which are often subtle and difficult to discover before the part fails (Sturm 2014)."

Therefore, after exploring the subject of cyber threats and the problems they may cause to vulnerable infrastructures, the next subsection focus on the existing building design practices, followed by the investigation upon the infrastructure supportive responsible for allowing the information flow.

4.3 Building Design Practices

Before starting the project process, it is essential to understand the project life cycle. The project life cycle can be represented in diverse stages due to their different purposes and deliverables. Thus, to illustrate this statement, here is mentioned the RIBA Plan of Work that is "still the definitive design and process management tool for the UK construction industry" [48]. The cited plan of work provides a framework for AEC professionals, especially for architects, in which these professionals can clarify for their clients all the content of the diverse stages of a project [48]. The plan of work is divided into seven different stages, as presented in Figure 26:

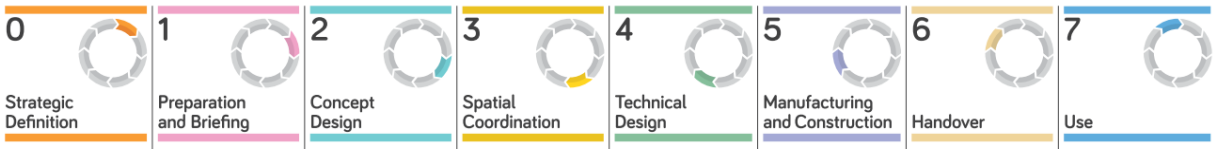

Figure 26: RIBA Plan of Work 2020. Source: RIBA [48]**.**

For this research study, here is considered only the fifth initial stages of the RIBA Plan of Work, focusing on Stage 4 (technical design). The fifth initial stages and their respective description is presented in Table 9:

Table 9: RIBA's five initial stages. Source: RIBA [48]**.**

Stage	Description
Stage 0 – Strategic Definition	to ratify that a construction project, or otherwise, is the best means of achieving the Client Requirements. (…) It focuses on making the right strategic decisions and capturing them in a Business Case.
Stage 1 – Preparation and Briefing	the client team begin the briefing process during Stage 1. (…) This stage is about developing the information that the design team will need to commence the design process at Stage 2.
Stage 2 – Concept Design	(…) sets the Architectural Concept for a project. Proposals that align with the Site Information and the Project Brief, including the Spatial Requirements, are prepared.
Stage 3 – Spatial Coordination	(…) is fundamentally about testing and validating the Architectural Concept, to make sure that the architectural and engineering information

	prepared at Stage 2 is Spatially Coordinated before the detailed information required to manufacture and construct the building is produced at Stage 4.
Stage 4 – Technical Design	(…) involves the preparation of all information required to manufacture and construct a building.

Moreover, it is essential to know how the project information is stored, managed and exchanged. Thus, this study considers that these activities are performed based on the BIM methodology. However, before the starting of the project design process, it is also essential to determine in which BIM maturity level the supplier and its supply chain will develop the project design. Here, it is considered that the building design practices are developed within the BIM maturity level number three. The maturity levels and their descriptions are presented in Figure 27:

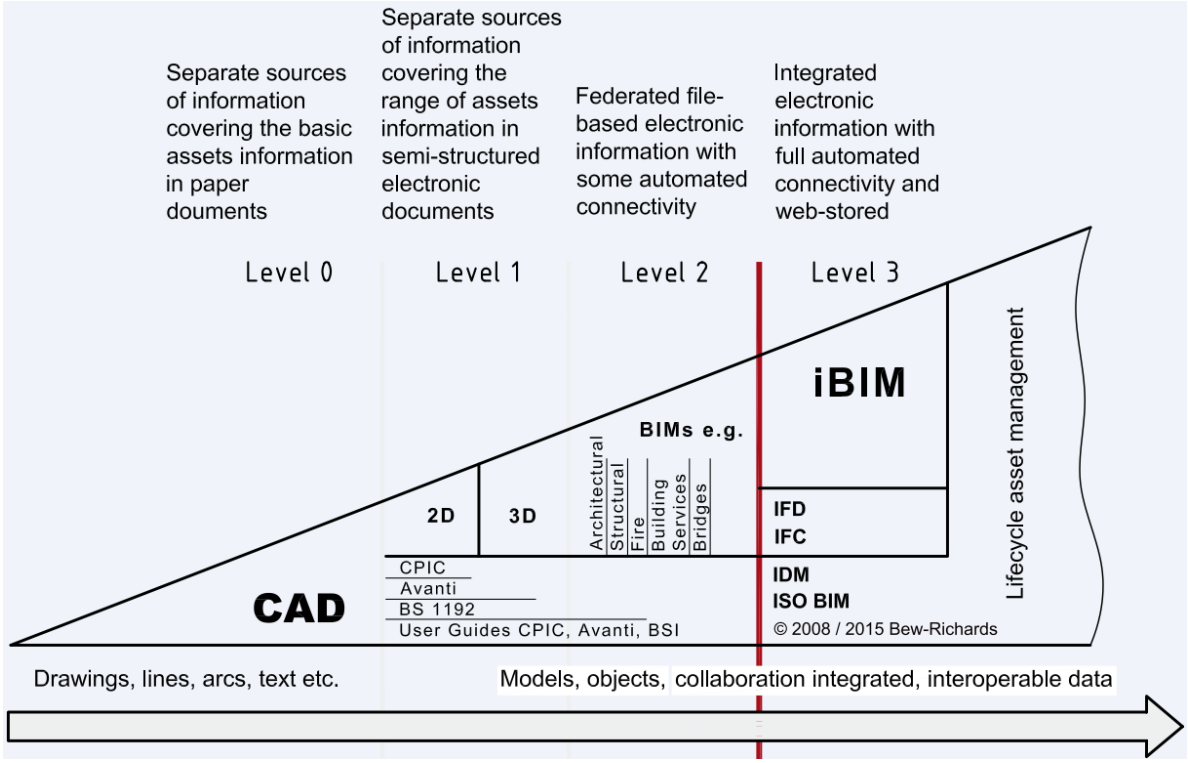

Figure 27: BIM maturity levels. Source: adapted from PAS 1192-5 [9]**.**

A supplier and its supply chain typically develop the project information process. In this case, the DEPEN is the public agency which is responsible for penal buildings projects.

According to Brazilian legislation, public building construction projects can be developed through two different ways: “direct” or “indirect” ones. The “direct” way is when the public agencies and entities have their personnel experts; oppositely, the “indirect” way is when a third party contracts the building construction projects through a bidding process [49]. The bidding process is presented in sequential order, following the steps below:

I. Bidding the preliminary phase;
II. Bidding internal phase;
III. Bidding external phase;
IV. Contractual phase; and
V. Bidding post-contractual phase.

The supplier and its supply chain that will develop the technical project design shall be chosen based on what is required by the bidding modality described on public notice. Here is considered the public tender bidding modality. The public tender "is the bidding modality among any interested parties to choose technical, scientific or artistic work, through the institution of awards or remuneration to the winners, according to the criteria set out in the notice published in the official press at least forty-five days in advance" [49]. This part corresponds to the second step (bidding internal phase) presented above.

Aligned with the ISO 19650-2 [50] and according to this particular research study, here is presented the interface between the parties: the client (DEPEN) and the public tender winner - supplier and its supply chain (Design company) - as illustrated in Figure 28:

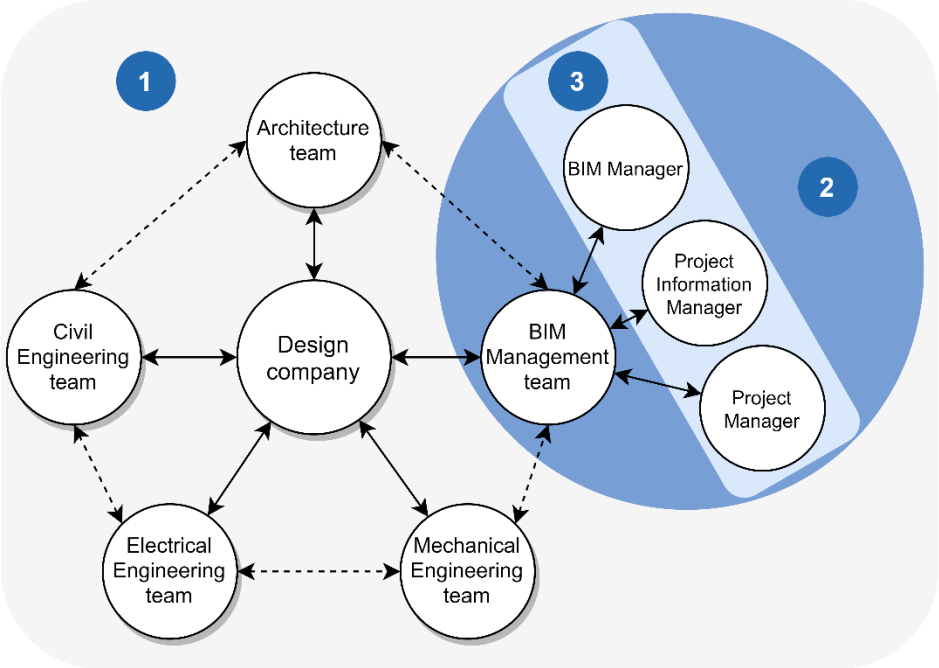

Figure 28: project team organization. Source: adapted from ISO 19650-2 [50]**.**

The image above, adapted from the ISO 19650-2 [50], shows the information as follows:

- Appointing party (Design company);
- Lead appointed parties (BIM Management team, Architecture team and others); and
- Appointed parties (BIM Manager, Project Information Manager, Project Manager, etc.).

Considering what demands the BIM maturity level 3 and the interface between parties, it is presented a simple scheme of project development and management, in Figure 29:

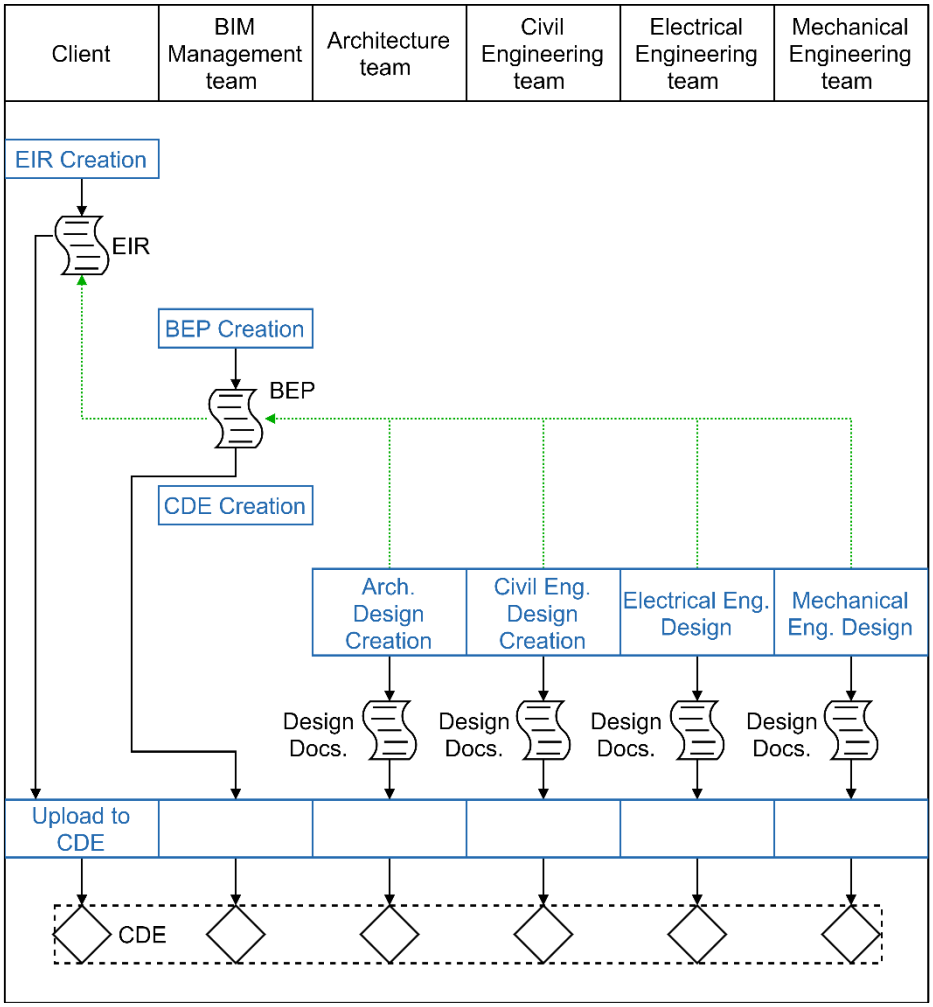

Figure 29: as-is design process map. Source: the author.

The supplier and its supply chain, presented in Figure 28, are responsible for producing the deliverables required by DEPEN on the EIR document, that is also a deliverable, shown in Figure 29. According to the ISO 19650-1 [10], the EIR "set out managerial, commercial and technical aspects of producing project information. The managerial and commercial aspects should include the information standard and the production methods and procedures to be implemented by the delivery team."

Having set out the EIR, the Design company elaborates the BEP documents – pre and post-appointment - that will guide the project teams to produce the deliverables answering the requirements presented in the EIR. The BEP is a "plan that explains how the information management aspects of the appointment will be carried out by the delivery team", conforming described in the ISO 19650-2 [50]. Other documents, as informed by the ISO 19650 on its part 1 and 2, are also part of the management process. However, they are not in focus. Besides, all the project deliverables shall be stored within a collaborative digital environment, identified in Figure 29 as "CDE".

Furthermore, infrastructure is necessary for project development and management. According to the online Oxford Learner's Dictionaries, "infrastructure" stands for "the basic systems and services that are necessary for a country or an organization to run smoothly, for example buildings, transport and water and power supplies." On the other hand, the online Cambridge Dictionary brings another definition which is more suitable to this research study: "the equipment, software, etc. that a computer system needs in order to operate and communicate with other computers."

Schematic infrastructure support for the project development could be: a "Start(ing)" point, corresponding to the collection and insertion of information (inputs), which is made by "Human Resources" and has its insertion made within "Cyber-physical Systems"; the "End" corresponds to the process outputs (deliverables), as illustrated in Figure 30:

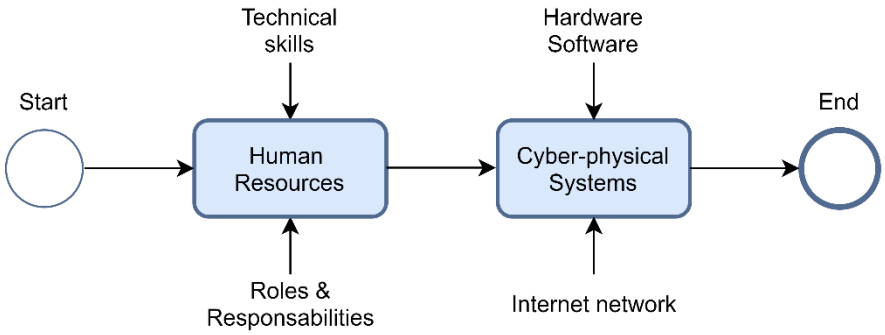

Figure 30: project development schematic infrastructure. Source: the author.

CPS are systems "designed as an entity, or set of entities, with a specific purpose, or to meet a capability objective" [9]. Furthermore, a complete definition of a CPS could be: "(…) integrations of computation, networking, and physical processes (Lee and Seshia, 2010), (Cárdenas, 2008). The key characteristic of cyber-physical systems is their seamless integration of both hardware and software resources for computational, communication and control purposes, all of them co-designed with the physical engineered components (Poovendran, 2010)" [51]. In this research study, the CPS, as presented in Figure 30, is understood as defined by the PAS 1192-5 [9] and Lun et al. [51].

Lun et al. [51] also add that "Among the many applications of CPS we can find high confidence medical devices and systems, assisted living, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, critical infrastructure

control (electric power, water resources, and communications systems for example), distributed robotics (telepresence, telemedicine), defense, manufacturing, smart structures, etc."

On this study, for a didactical purpose, the Cyber-physical systems presented in Figure 30 are dismembered into two more systems (Physical Systems and Digital Systems), as shown in Figure 31:

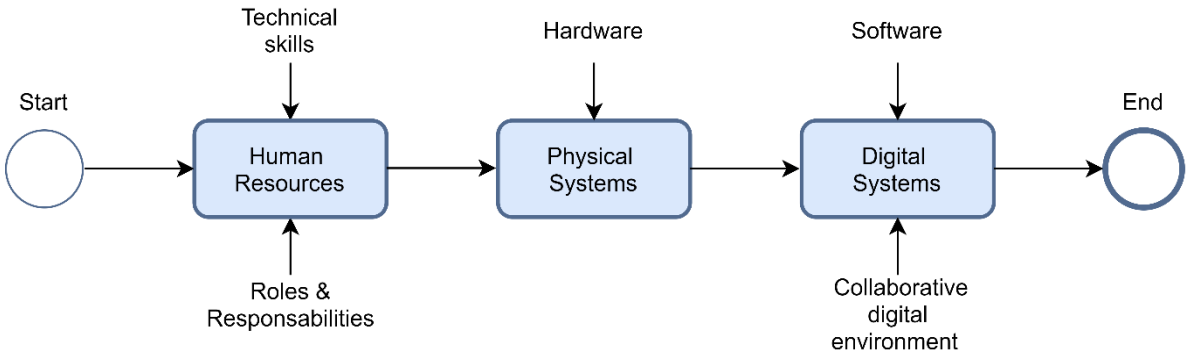

Figure 31: dismemberment of the schematic infrastructure. Source: the author.

The criticality of this infrastructure is analysed on the next subsection.

4.4 Critical Infrastructure

This subsection analyses the infrastructure necessary for the development of the project information process informed on the subsection "Building Design Practices". First, it is started with a semantical analysis of the term "critical"; then, it is chronologically explored the diverse definitions for critical infrastructure. Finally, it is explained about the criticality of the infrastructure referred to this research study.

The word "critical" can be characterized as: "extremely important because a future situation will be affected by it" (online Oxford Learner's Dictionaries). Yet, the online Cambridge Dictionary brings another definition for it: "extremely important to the progress or success of something."

There is a wide range of definitions for "critical infrastructure", being developed according to local circumstances, time-based specific facts and the understanding of each nation. The diverse explanations for critical infrastructure are further explored with the purpose to realize how the term has evolved as time passes.

According to Moteff et al. [52], the first version of the American National Plan for Critical Infrastructure defines critical infrastructures as "those systems and assets - both physical and cyber - so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety."

Again, about the criticality of the infrastructure, Moteff et al. [52] give us an idea mentioning that "After identifying what may be considered a critical infrastructure, a protection strategy must identify which

elements of the infrastructure are critical to its function or pose the most significant danger to life and property. Not all assets may be critical, and some may be more so than others. However, the size and complexity of these infrastructures can make identifying which assets of an infrastructure are critical a daunting task."

According to Church et al. [53] words, critical infrastructure "can be defined as those elements of infrastructure that, if lost, could pose a significant threat to needed supplies (e.g., food, energy, medicines), services (e.g., police, fire, and EMS), and communication or a significant loss of service coverage or efficiency."

In line with the words of Murray et al. [54] the Executive Order 13010[19] from the White House (U.S. Government), informs that "Basic inventories of critical infrastructure are often subdivided into sectors, and include (…): telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government."

Besides, Egan [55] catches one's attention for the necessity to understand the "criticality" of infrastructure, in order to predict its vulnerability. Predicting the system's vulnerabilities is an essential tool for risk mitigation, because as mentioned by Auerswald et al. (2006, cited by Egan, 2007), "If an organization can predict vulnerabilities before they emerge, it can make its own (endogenous) changes to account for them."

As mentioned by Aradau [56], the UK Centre for the Protection of National Infrastructure informs that "Definitions of critical infrastructure list heterogeneous elements, from communications, emergency services, energy, finance, food, government and health to the transport and water sectors (Centre for the Protection of National Infrastructure, 2009)." Later on, the author also says that: "Unlike the protection of citizens, critical infrastructure is mainly concerned with physical and cyber-based systems" [56].

Conforming to Yusta et al. [57] "(…) the term 'critical infrastructure' is defined as any element, system or part thereof, situated in a state that is considered essential for the maintenance of vital societal functions, health, physical integrity and security, social and economic welfare." The authors also mention the concept about critical infrastructure through the words of Hull et al. (2006): "The concept of critical infrastructure and key resources includes all assets that are so vital for any country that their destruction or degradation would have a debilitating effect on the essential functions of government, national security, national economy or public health."

[19] U.S. President's Commission on Critical Infrastructure Protection (PCCIP) (E.O. 13010)

Besides, a recent definition of critical infrastructure can be found in the words of Pärn & Edwards [11] when referring to a CDE cybersecurity adaptation: “the processes, systems, technologies and assets essential to economic security and/or public safety.”

Therefore, considering what was exposed, for this research study “critical infrastructure” is understood as: “fundamental framework of interdependent networks and systems that provide reliable information flow and services essential to the progress or success of an organization, which incapacity or destruction would have a debilitating impact on it.”

With the purpose to perform a risk assessment, first, it is necessary to understand its criticality. Thus, the schematic infrastructure shown in Figure 31 can be represented by a larger system that has its framework (small systems). Besides, each small system is considered as an asset for the organization. This organization is illustrated in Figure 32:

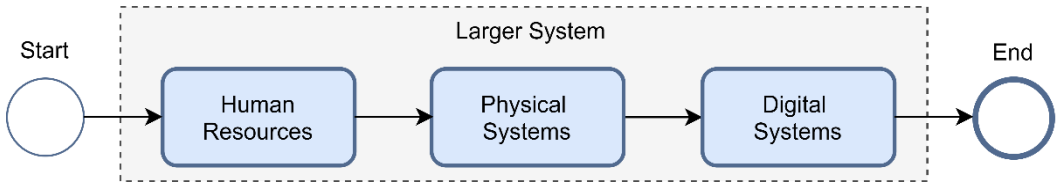

Figure 32: systems as assets. Source: the author.

The “Human Resources” corresponds to the supplier and its supply chain that are responsible for the project development.

Physical systems here are understood as “hardware”, which are “the machines and electronic parts in a computer or other electronic system” (online Oxford Learner's Dictionaries), i.e. laptops, desktops, pen drives, USB drives, memory cards, mice, keyboards, modem, printers and others, for example. They correspond to the physical devices that are used by the professionals to develop the project.

On their study about hardware and software co-design, Jerraya et al. [58] state the systems as »digital systems«, classifying them by their main domain of application, also affirming that they can be geographically distributed. Figure 33 illustrates their viewpoint:

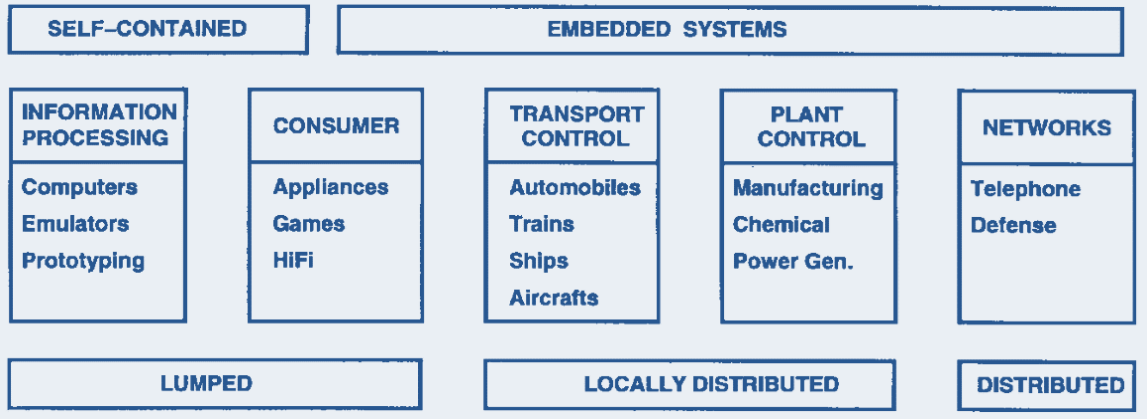

Figure 33: some application domains of electronic systems. Source: adapted from Jerraya et al. [58]**.**

Along with the study, the authors mention that "The design of hardware/software systems involves modeling, validation, and implementation", where modelling can be defined as "the process of conceptualizing and refining the specifications, and producing a hardware and software model." Further, they call validation as "the process of achieving a reasonable level of confidence that the system will work as designed (…). Regarding implementation, they call it as "(…) the physical realization of the hardware (through synthesis) and of executable software (through compilation)" [58].

Besides, as working practices are quickly evolving, better performances have been required from hardware's systems. Hence, hardware companies are developing studies and applying more time with the purpose to enhance tools that can meet the designers' need. Furthermore, it has a high monetary value, by the way.

The devices' high prices can be understood since 1997 when, according to Jerraya et al. [58], "The forecast of the worldwide revenues of integrated circuit sales (…) explains the high demand of electronic system-level design tools, whose volume of sales is expected to grow at a compound annual rate of 34% in the 1993–1998 time frame (…)." They also add information about another kind of value than the one of production, when they say that "hardware (e.g., cores) and software (e.g., microkernels) can be viewed as commodities with large *intellectual property* values." The question is: how high could be the financial cost for the company if it suffers a malicious attack? The answer is high, very high.

Oppositely to the last subject, "Digital Systems" here is understood as "software", which are "the programs used by a computer for doing particular jobs" (online Oxford Learner's Dictionaries). According to the report of The U.S. Council of Economic Advisers [59] about the expenditures from malicious cyber activities, a computer's software "is any data or computer instructions stored on a computer's hardware. Software is encoded in a binary basis and forms the tools by which computers execute tasks and manipulate information."

There is a bunch of software that help the supplier and its supply chain to produce the client's required deliverables. Software programmed to let information in, allow their modelling, storage, management and exchange (with almost no losses) have been being part of the work adaptations performed by professionals.

Aligned with the idea of adaptations and implementations at work, the RIBA Plan of Work [48] mentions the challenges of choosing the most appropriate design tools, as the Civil Construction professionals are adopting "(…) transitions from traditional design and construction processes", with the purpose to enhance their productivity. The document informs that "The challenge for those considering how to incrementally develop their workflow in future will be in determining which of the many digital tools and technologies will be most appropriate for how they want to work." The document also informs about technologies that possibly will be part of the professionals' design tools, which are presented in Table 10:

Table 10: source: adapted from the RIBA Plan of Work [48]**.**

Technology	Description
Rules-based design	Design automation is possible where detailed rules for spaces, adjacencies and building systems can be determined by repeat clients.
Generative design	By using complex coding scripts, it is possible to generate a multitude of design options instantly.
4D	(…) 4D (3D plus time) tools are primarily being used (…) during the tender process to unlock the most efficient way of manufacturing and constructing the building (…). 4D tools also enable contractors to convince the client team that their proposals are robust and realistic.
5D	5D enables the addition of the cost dimension to 4D information.
Integrated system analysis	When available, engineering analysis software that provides real-time contributions to the architectural development will make the design process more accurate, saving design time and, crucially, allowing design decisions to be based on high-quality data.
Manufacturing workflow	Designing for manufacturing and assembly (DfMA) is rapidly being seen by clients as the way to transition towards faster and more effective ways of making buildings, and by contractors as a way to lower the costs of delivery and reduce risks.
Artificial intelligence	Holding large databases of projects will enable clients or designers to begin to use their models and information more effectively, but consistent classification and other factors will be crucial in making AI work. In the long term, it is inevitable that AI will drive new ways of designing, and of making the connections necessary to drive better client outcomes.

Note: the complete information about each mentioned item may be checked within the RIBA Plan of Work document.

Besides, there is a variety of digital tools (part of the design and management processes) which are also supportive for the design team that uses for planning and communication such as e-mails exchange, planners, calendars, web-based platforms and others.

Furthermore, among the technological tools, there is the CDE which is at the discussion-centre of this research study. Considering the CDE as part of the project management and its infrastructure, special attention shall be given to its extraordinary proprietary value. Besides, it also has an economic benefit for the involved actors/organizations, considering that all the information from the digital asset is supposed to be stored within this collaborative digital environment.

On this study about the "cyber security issues inherent in Level 2 BIM in the UK", Boyes [21] highlights the attention that must be given to the CDE, principally to its contents: "This has information management implications, including the need for appropriate governance and a curator role to maintain data quality and integrity on behalf of the asset owner and users." He also adds that isolated information sources within the CDE may not be sensitive, however "(…) certain combinations of information sources when taken together may significantly increase sensitivity."

Aligned with that, Pärn and Edwards [11] mention on their study that the "Adaptation of a CDE for critical infrastructure (i.e. the processes, systems, technologies and assets essential to economic security and/or public safety) constitutes a key facet of effective asset digitalization and offers potential "long-term" lifecycle savings for both government and private sector funded projects (Bradley et al., 2016)." The authors also inform that "However, the proliferation of cyber-physical connectivity inherent within a CDE has inadvertently created opportunities for hackers and terrorists, and an omnipresent threat of cyber-crime prevails (Boyes, 2013a) (…)."

Pärn and Edwards [11] continue saying that "Significant risks posed could disrupt the stream of virtual data produced and in turn, have a profound detrimental impact upon a virtually enabled built environment, leading to physical interruption and/or destruction of infrastructure assets (e.g. electricity generation) thereby endangering members of the public". Furthermore, some illustration is given by the authors regarding the cyber vulnerabilities of a CDE environment, as shown in Figure 34:

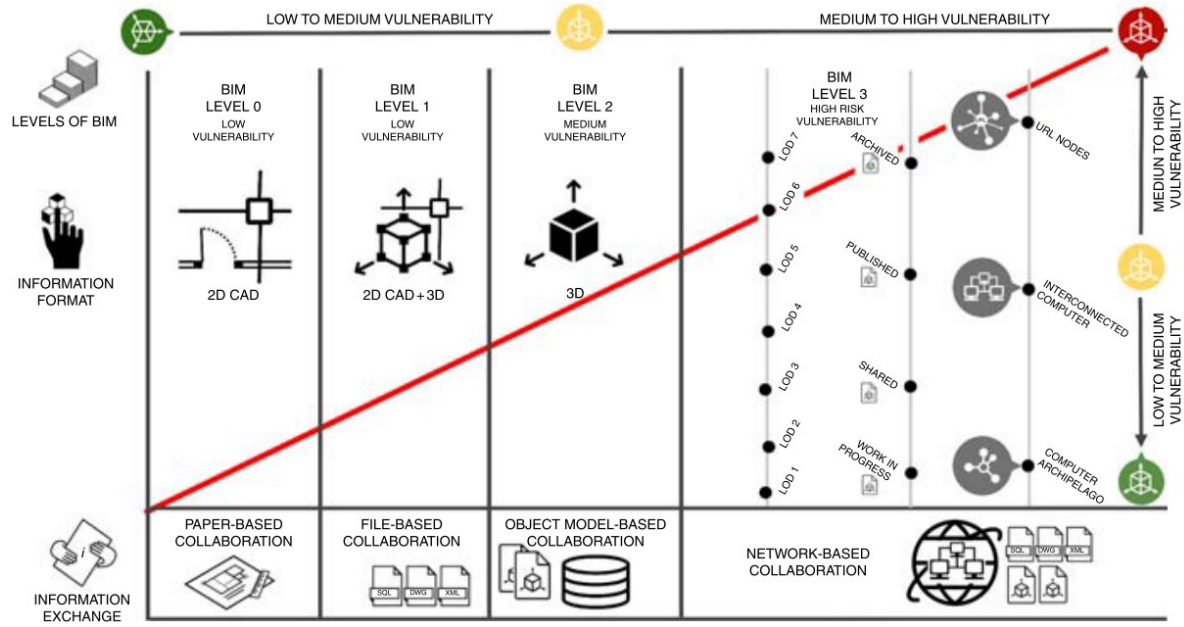

Figure 34: cyber vulnerabilities of the CDE environment. Source: Pärn and Edwards [11]**.**

It is interesting to observe, from the Figure 34, that the authors separate the vulnerability risk into two fields: “low to medium vulnerability” (left) and “medium to high vulnerability” (right). Besides, it can also be checked that in each field there is the presence of a different BIM level, where the initial BIM levels belong to the left-field and the BIM level three belongs to the right area, i.e. is more vulnerable to cyber threats. The fact that the BIM level three depends more on the network-based collaboration is preoccupant because there is the imminent cyber risk involving both the physical and digital systems.

Going further, checking what is newest about cyber threats, recently it was concluded that a malware that encodes binary information named “AiR-ViBeR” could exfiltrate data “from air-gapped computer to a nearby smartphone on the same table, or even an adjacent table, via vibrations”, according to Guri [60].

The next chapter presents an approach to general solutions that can be applied against informed security threats.

5 CYBERSECURITY MEASURES

This chapter informs about general cybersecurity measures against cyber threats and cyber-attacks. First, it is presented an overview of cybersecurity measures that have already been taken/indicated by some organizations. Next, it is commented about the cyber-resilience subject, informing the importance of the organization systems' recovery after security failure. Then, it is indicated some security propositions to cybersecurity.

5.1 Overview

Providing security measures to guarantee the integrity of the digital environment is of vital importance for the company. On the contrary, the company can suffer a significant loss, not only regarding data but also about money, time, intellectual property and, in extreme cases, also human lives.

Before starting to think about the cybersecurity measures, it is necessary to understand what previous studies have already reported about the subject. Hence, this subsection presents information about the topic, through a chronological development and based on different viewpoints.

On their study about "methodologies and applications for critical infrastructure protection«, Yusta et al. [57] presents a critical infrastructure framework protection elaborated by the USA Department of Home Security, that can be seen in Figure 35:

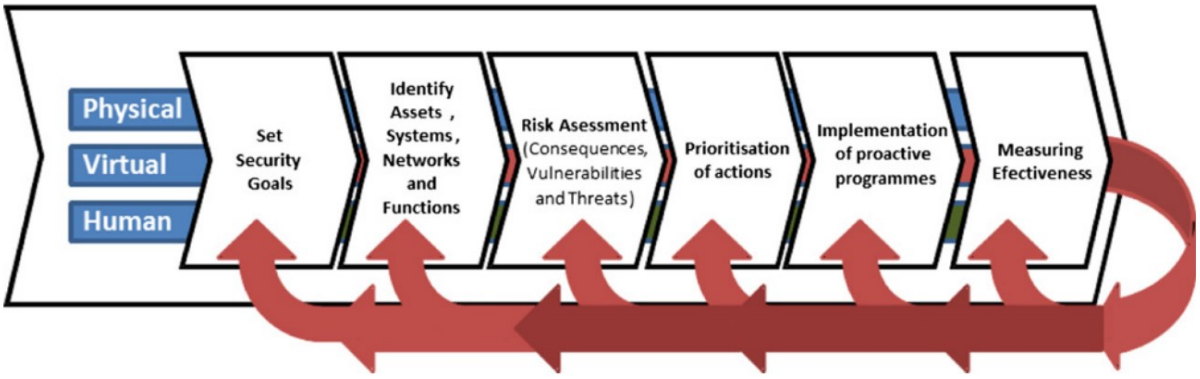

Figure 35: a framework for the protection of critical infrastructure and key resources. Source: Yusta et al. [57]

From the picture above, the step-by-step of the framework has the following sequence:

1. To set security goals;
2. To identify assets, systems, networks and functions;
3. To make a risk assessment;
4. To prioritise actions;
5. To implement proactive programmes; and
6. To measure effectiveness.

Aligned to what was elaborated by the USA Department of Home Security, the UK National Cyber Security Centre [61] also presents some steps to cybersecurity protection which can be seen in Table 11:

Table 11: ten steps to cybersecurity. Source: adapted from UK National Cyber Security Centre.

Security areas	Description
Set up your Risk Management Regime	Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.
Network Security	Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.
User education and awareness	Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.
Malware prevention	Produce relevant policies and establish anti-malware defences across your organisation.
Removable media controls	Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.
Secure configuration	Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.
Managing user privileges	Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
Incident management	Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.
Monitoring	Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.
Home and mobile working	Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

As mentioned by Yusta et al., the PAS 1192-5 [9] also brings information about risk assessment, affirming that "Good security requires holistic risk assessment and applying the principles of proportionality to achieve an appropriate balance of the costs and constraints associated with protecting an asset versus the impact that its loss, compromise or failure can have on the organization and the organization's stakeholders."

Further, The UK National Cyber Security Centre, on another issued document, informs about good practices on how to deal with cyber-attacks, informing that "Preventing, detecting or disrupting the attack at the earliest opportunity limits the business impact and the potential for reputational damage. Once the attacker has consolidated their presence they will be more difficult to find and remove" [46]. Later on, the document also informs how to reduce the exposure to cyber-attack, summarized below:

- Breaking the attack pattern;
- Reducing the exposure using essential security controls: establish network perimeter defences, malware protection, patch management, whitelisting and execution control, secure configuration, password policy, user access control, security monitoring, user training education and awareness and security incident management;
- Mitigating the stages of an attack; and
- Raising cyber defences.

Thames and Schaefer [5], aligned to what was informed by Boyes [21] about the traditional information security triad, say that it is security mechanisms together with "authenticity, access control and non-repudiation" that prevent computer and network intrusions and attacks. On the same document on their article about digital manufacturing, Wegner et al. call the attention for the necessity of having a single point of failure as one of the possibilities by adopting a new security approach.

Mr Bunker, a cybersecurity expert at the ENISA, on an interview about cybersecurity and IoT themes for The Telegraph, informed that things are improving regarding cybersecurity as technology companies are "making efforts to tighten up security" [4]. Mr Bunker adds that "'In the same way that individuals have been told about the 'dangers' of social media, so too they need to be told about sharing and protecting the information from IoT devices'."

The IOCTAC report [6] presents a seven-step OSINT and Tactical Coordination plan, regarding the combat against cyber threats, described below and illustrated in Figure 36:

1. Early detection and identification of a major cyber-attack;
2. Threat classification;
3. Emergency response coordination centre;
4. Early warning notification;
5. Law enforcement operational action plan;
6. Investigation and multi-layered analysis; and
7. Emergency response protocol closure.

Figure 36: OSINT & Tactical Coordination. Source: adapted from Europol [6]**.**

Nevertheless, despite information regarding critical infrastructure and cyber-attacks and threats, there is an important theme to be explored: the resilience of the systems and the organization of the supply chain. Therefore, the next subsection presents the concept of resilience and its application for cyber environments.

5.2 Cyber-Resilience

Based on a semantical analysis, the online Oxford Learner's Dictionary informs that resilience means "the ability of a substance to return to its original shape after it has been bent, stretched or pressed." The meaning of the word brought by the dictionary is more specific and related to the dimensional characteristics of a substance. Oppositely, the online Cambridge Dictionary has a more general approach defining it, informing that resilience is "the quality of being able to return quickly to a previous good condition after problems."

Going to a more contextualized approach, according to Boyes [41], resilience "is the ability to adapt and respond rapidly to disruptions and maintain continuity of business operations." He also advises on how to proceed with the disruptive problems and the resilience of the system when he says that the personnel involved in a determined work "should have considered potential causes of disruption, both human and natural, make sure that key systems and processes are maintained to ensure business continuity, and have in place systems and processes to enable timely detection of, and response to, disruptive events."

In a compilation of articles on Cyber-Resilience in Supply Chains, Adrian Davis [62] brings the definition of Peck et al. (2003) that fits his work as well to this research study, informing that resilience is "[…] the ability of a system to return to its original [or desired] state after being disturbed (Peck et al., 2003)."

Along with the study of Adrian Davis [62], he says that, in order to build cyber-resilience across the supply chain, the organization needs "to build a set of capabilities, both internal- and external-facing". He also presents a material published by the World Economic Forum, on how to deal with the cybersecurity subject, mentioned here:

1. Implement a cybersecurity (or information security) governance framework and place a member of the executive management team at its head.
2. Create a cybersecurity programme.
3. Integrate the cybersecurity programme with enterprise risk management approaches.
4. Communicate, share, and apply the cybersecurity programme with suppliers, educating them where necessary.

Luca Urciuoli [62], on this same compilation of articles on Cyber-Resilience in Supply Chains, enumerates some strategies to manage resilience that he found during his research:

1. Diversification of suppliers;
2. Inventory management;
3. Ensure additional transport capacity and multiple consignment routes;
4. Product-centric design; and
5. Information sharing.

On another study from 2015, Boyes [63] mentions a definition on cyber-resilience informed by the World Economic Forum (WEF, 2012), which is "the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery".

Understood the cyber-resilience meaning and its applicability, the next subsection shows some propositions on cybersecurity.

5.3 Propositions to Cybersecurity

This subsection presents some propositions on cybersecurity made by some experts after their analysis on cyber-attacks and threats on cyber-physical systems. The information is presented chronologically as a common strategy of this research study.

About the sensitive information that may be stored within a CDE, Boyes [21] on his study calls the attention for the control mechanisms regarding the interoperability activities between the different

models stored in the CDE. He says that "In addition to the configuration control mechanisms, the information manager must also address potential interoperability issues between different models held within the CDE."

Through a compilation of articles on the same book, it is presented the authors' experiences dealing with the cybersecurity issue, in order of appearance.

Cai et al. [5], develop a study about an encryption approach "to support product development collaboration". They emphasize the necessity of data encryption, affirming that it is essential that the "information protection in a network environment." They also add that "Data encryption is an important approach for information hidden in network. It can ensure that the hidden information cannot be obtained by unauthorized users. In recent years, the encryption methods have been widely used for multi-media data, such as the image encryption."

Despite this study discusses cybersecurity measures upon buildings, it takes a look into a big data security intelligence system addressed to the healthcare industry, in a study developed by Manogaran et al. [5]. The authors present another aspect of data encryption and the vulnerabilities regarding it, when they say that "In general, simply encrypting data and using the non-secured protocol can enable confidentiality but not ensure the data integrity." Later on, the authors cite a security algorithm, which can protect from the access of an unauthorized user the application which is within a cloud.

Moreover, Manogaran et al. [5] also propose a secure IoT architecture "to store and process scalable sensor data (big data) for health care applications." Thus, along with their study, they present information on components in IoT, their vulnerabilities, types of cyber threats and attacks as well as available security requirements with the purpose to solve the problems. This compilation of data can be found in Table 12:

Table 12: various security requirements and solutions in components of IoT. Source: adapted from Manogaran et al. [5]**.**

Components in IoT	Available security requirements and solutions
Physical objects in IoT	• Encryption/Cryptographic techniques • Continuously evaluates the suspicious nodes' behaviour can reduce the influence of malicious user access • Authentication • Authorization • Access control • Identification
Communication technologies in IoT	• Communication security: Security algorithm and protocols used to provide smoothness transitions connections among different edge networks • Encryption/decryption is used to provide confidentiality service

	• Strong authentication also used to provide security solutions • Backup solution is used when network fails • IoT communication protocols enhancement also increase the security • Authorized access and Availability
Applications of IoT	• Data separation is used between information content and information source • Encryption/decryption mechanisms • Secure data access • Confidentiality of data • Secure sensitive data • Backup plan • Proposing traditional distributed database technology • Scheduling techniques • Assuring identification • Assuring authentication • Firewall and antivirus • Intrusion detection • Enhanced communication protocols security

The proposed security system by Manogaran et al. [5] uses the authorization and authentication processes, as shown in Figure 37:

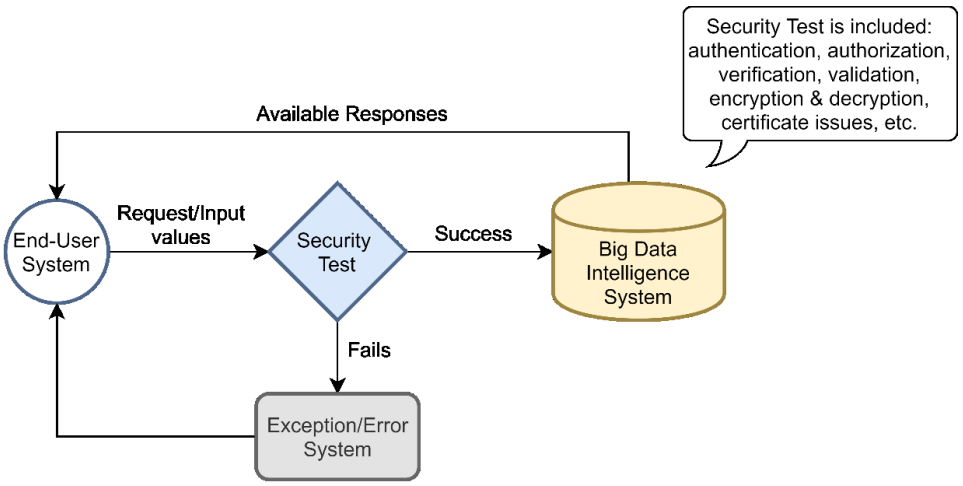

Figure 37: flow diagram for the proposed system. Source: adapted from Manogaran et al. [5].

From the figure above, it can be inferred whether the end-user tries to request and/or input values on the BDIS, he/she will pass by a security test. If there is a success on the attempt, the end-user is able to access the BDIS; otherwise, the access is denied and, the fault passes through an exception/error system which returns to the end-user system. The idea to install/design a security test is interesting, principally if its content is based on responses related to specific topics that just the authorized person to access the system would know.

Glavach et al. [5], on their article, present cybersecurity threats related to the DDM community and potential scenarios and possible motivations. Besides, they also present protocols and recommendations for incorporating best practices during system installation and its posterior operation. Later on, they mention that the strategy for DDM risk management is the same as the one applied for the traditional risk management processes "at each component and along the entire digital thread." Thus, they enumerate some steps for risk management:

Step 1: Identify the risk. Identify vulnerabilities and threats with a potential for loss to availability, integrity, confidentiality. Vulnerabilities are defined as a weakness or likely deterioration in security. Threats are defined as an exploitation of a security weakness.

Step 2: Analyze the risk. Determine the likelihood and impact of each risk by developing an understanding of the risk, impact to the specific digital thread and the potential to affect the entire digital thread.

Step 3: Evaluate the risk. Evaluate the risk by determining the risk magnitude, (the combination of likelihood and impact), technical control to minimize risk or categorized the risk as acceptable.

Step 4: Risk Controls. Risk control is the process of implementing controls or documenting acceptable risk for future evaluations

Furthermore, at the conclusion of their article, they present a discussion of focus areas for DDM cybersecurity staff, with the purpose to mitigate cyber risks, as shown in Figure 38:

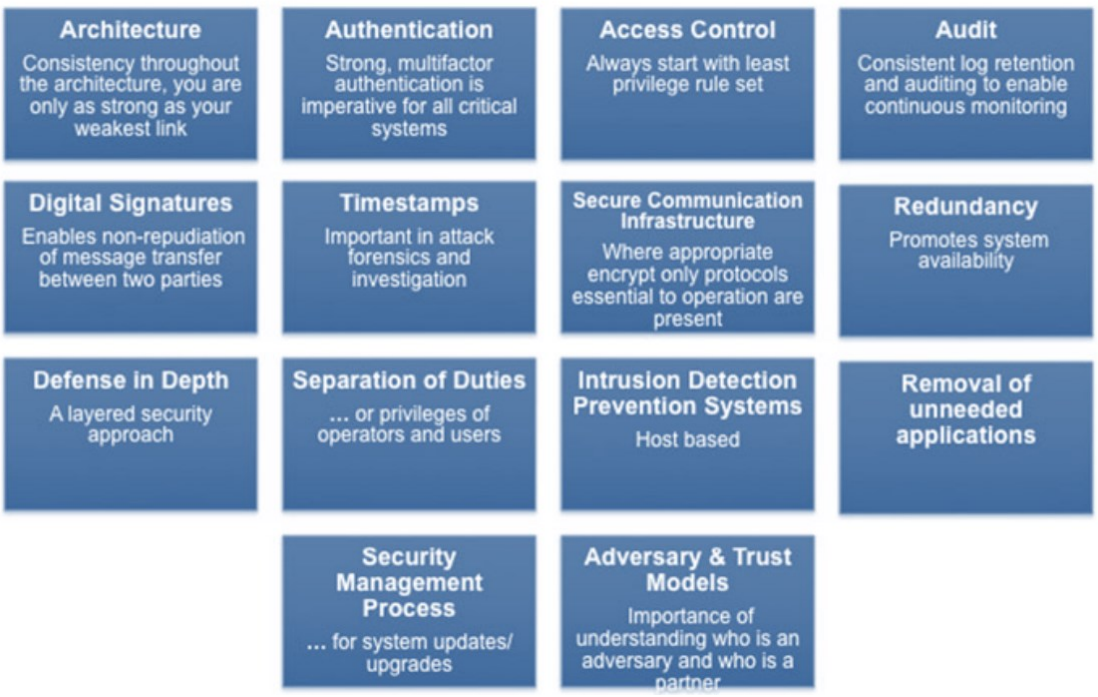

Figure 38: focus areas for the security team. Source: adapted from Glavach et al. [5].

They also add it must be identified and addressed "high-impact quick mitigation risks and position DDM systems on networks that preserve integrity, availability, and confidentiality of data" [5].

Confirming the idea to use an algorithm for security issues mentioned before, Thames and D. Schaefer [5] inform that "Cyberattack detection systems require algorithms that collect and analyze data generated by various events occurring within a cyber environment. The objective of a detection algorithm is to accurately discover suspicious activities based on the analysis of event data."

Besides, the study of Mantha & Soto [3] when investigating the cybersecurity issues addressed to the AEC industry they mention that it is fundamental to take into consideration the cybersecurity for the "transition into digitalization of the AEC industry". Besides, one focus of their study is to "develop a framework which academicians and construction professional can use to systematically identify cybersecurity risks."

Mantha & Soto [3] mentions that "The overall objective of the proposed framework is to identify avenues in which construction-related data could be directly or indirectly manipulated. (…). That is, identifying these avenues form a primary step to assessing the outcome (e.g., cost of a data breach) of these vulnerabilities, and subsequently devise action plans (e.g., the cost to improving the security of the systems) to address them. Initially, the framework structure is discussed in the context of interactions between stakeholders in a construction project and between connected construction sites. Then, information exchange channels are detailed from a project level to site level." Figure 39 presents the proposed framework:

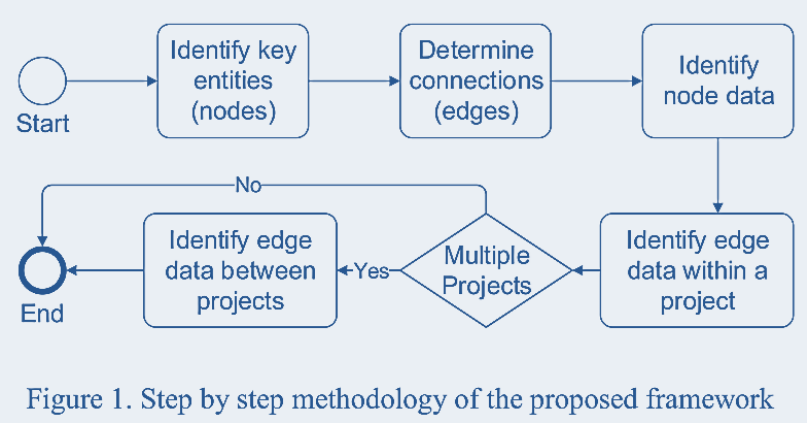

Figure 39: a framework to identify cybersecurity risks in the construction industry. Source: adapted from Mantha & Soto [3]**.**

Later on, the authors describe a »flow of data between the nodes (i.e., along the edges), at the nodes, and across the supply chain.« Figure 40 presents this flow:

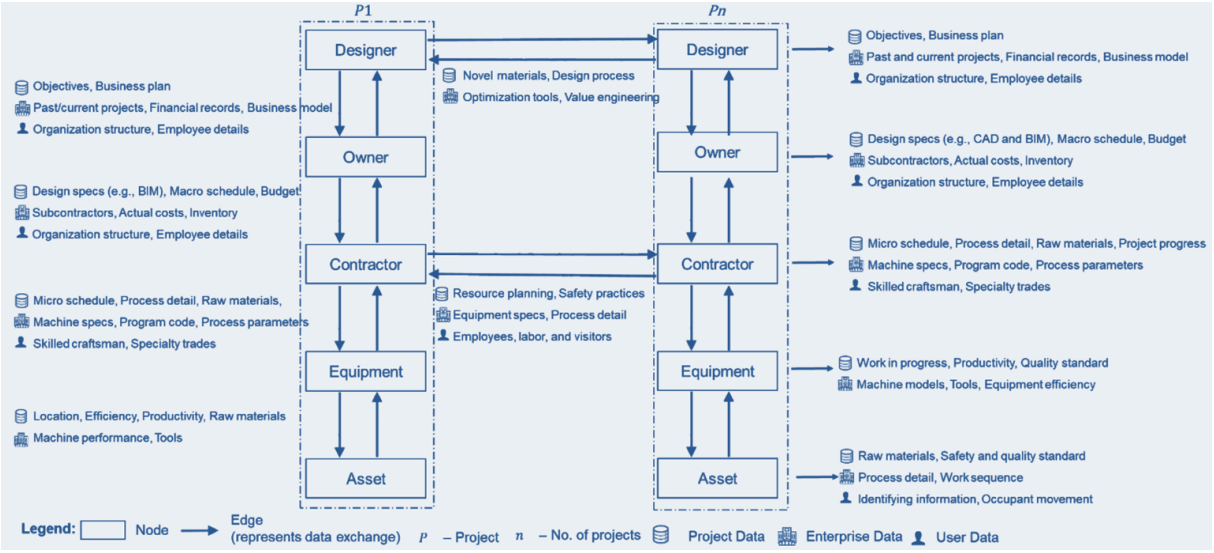

Figure 40: flow of data between the nodes. Source: adapted from Mantha & Soto [3]**.**

Another key-point that can be explored is the possibility to design the threat action, as it was made recently by a group of researches. The ESET[20] researchers have recently discovered (2020) a "previously unreported cyber espionage framework they dub Ramsay". According to the company's website "The framework is tailored for collecting and exfiltrating sensitive documents from air-gapped systems that are not connected to the internet or other online systems. Since the number of victims so far is very low, ESET believes that this framework is under an ongoing development process". Their findings resulted in an illustrative image (Figure 41) showing the different malware versions:

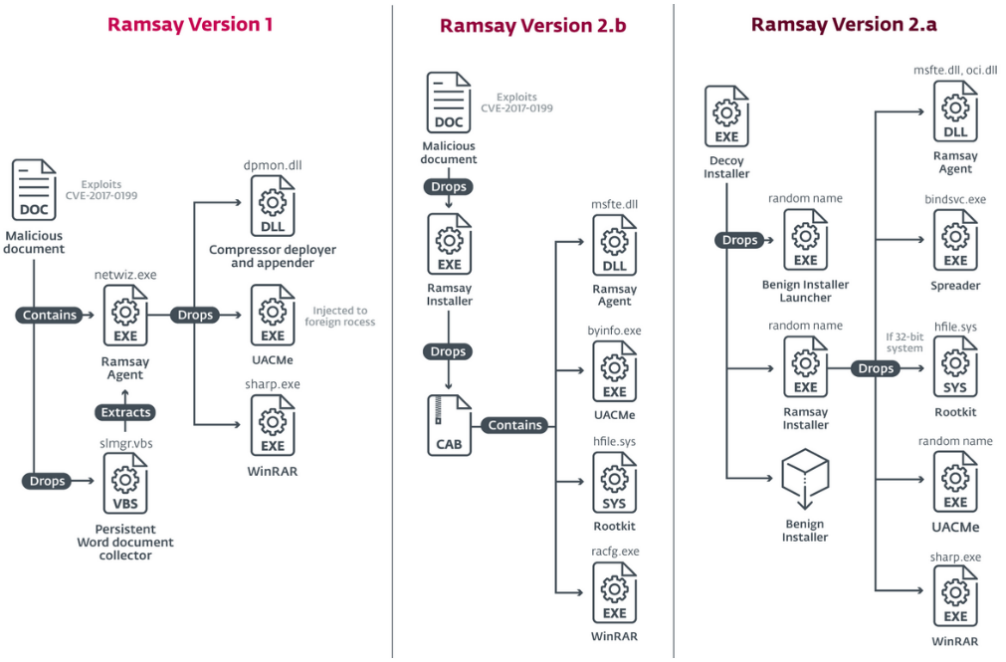

Figure 41: an overview of discovered Ramsay's versions. Source: ESET Company website.

[20] ESET is an »antivirus protection, creating award-winning threat detection software« company. Website: https://www.eset.com/au/

After presenting the mentioned propositions on cybersecurity, the next chapter establishes the vulnerabilities of the infrastructure of the penal buildings project design phase to cyber threats, suggesting the application of cybersecurity measures.

6 ANALYSIS

This chapter analyses the cybersecurity measures that can be applied to mitigate security risks involving the infrastructure of the penal buildings project design phase. Therefore, first, it shall be presented the CDE vulnerabilities. Next, it presents a Cybersecurity Protocol, which shall determine strategies to mitigate the security risks.

6.1 CDE Vulnerabilities

Pärn and Edwards [11] consider that the CDE vulnerabilities are more connected with the Cyber-physical systems of the infrastructure necessary for enabling the information flow. However, this study presents something beyond what was stated by the mentioned authors. The CDE vulnerabilities are directly related to the criticality of the whole infrastructure of the building design process, i.e. it embraces the "Human Sources", the "Physical" and the "Digital" systems. Thus, protecting the whole infrastructure is a way to assure protection for the CDE. In this line, from the "SECURITY CHALLENGES" chapter it was investigated the malicious agents and the cyber threats that could take advantage from the vulnerabilities of the infrastructure supportive for the penal buildings project design process. From this investigation, it is presented the following summary-table:

Table 13: systems' vulnerabilities. Source: the author.

System	Human Resources	Physical System	Digital System
Type of threat or attack	Interception of Communications; Homicide; Murder, Manslaughter; Bodily Harm and Acts and Omissions Causing Danger to the Person; Assaults; Kidnapping, trafficking in Persons, Hostage Taking and Abduction; Defamatory Libel; Hate Propaganda; Loss or disclosure of intellectual property; Loss or disclosure of commercially sensitive information; and Release of personally identifiable information.	External/Removable Media; Attrition; Loss of theft of equipment; Sabotage; and System failure.	Attrition; Improper Usage; Loss or Theft of Equipment; Cross-Site Scripting; Denial-of-Service/Distributed Denial-of-Service; Malware; Pishing/Spear Pishing; Passive Wiretapping; Spamming; Spoofing; SQL Injection; Scanning; Fingerprinting; Footprinting; Sniffing; Social Engineering.

For the risk analysis of the "Human Resources" system, it is considered the Canadian Criminal Code[21] [64] and selected the information most suitable for this research study. The research study focused on two parts of the Criminal Code, being them: Part VI, which informs about Invasion of Privacy; and Part VIII, which informs about Offences Against the Person and Reputation. As it can be realized, Human Resources might be exposed to "Invasion of Privacy" and "Offences Against the Person and Reputation", themes that suggest life-risk security.

Therefore, from the investigation of the systems' vulnerabilities performed before, it is realized the necessity to provide a risk mitigation process. Thus, the next subsection presents the proposition of a cybersecurity protocol.

6.2 Cybersecurity Protocol

Adapting the meaning of "protocol" given by the online Oxford Learner's Dictionary for this study, this subsection presents a set of rules and security procedures for protecting the infrastructure and, consequently the CDE, presented at the "Critical Infrastructure". The Cybersecurity Protocol is established as follows:

1. **Cybersecurity Team**. The establishment of a "Cybersecurity Team" by the supplier. The Client/Employer can request it from the supplier, or the supplier can do it without being asked to do so. One of the roles of the Cybersecurity Team is to keep personnel identification data secret and under control. Figure 42 illustrates it:

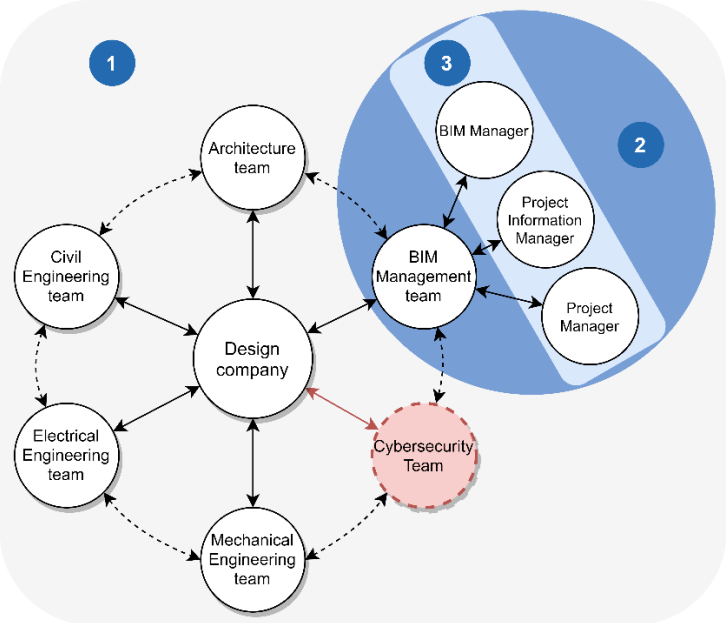

Figure 42: cybersecurity team. Source: adapted from ISO 19650-2 [50]**.**

[21] It was chosen considering that the country occupies the 13th position at the HDI rank, presenting the index of 0.922, according to the UNDP, inferring that the country may be an example of law enforcement.

2. **Risk Management Strategy**. To design and implement a risk management strategy to: identify, analyse, evaluate and control the risks [4]. The risk management strategy can also predict a) definitions for cybersecurity solution, applicable for the entire organisation's infrastructure; and b) application of cybersecurity solution;
3. **Cybersecurity Documents**. The establishment of manuals/guides addressed to cybersecurity, which informs about cybersecurity "good practices". The cybersecurity "good practices" may also be introduced through periodically workshops and training;
4. **Cybersecurity Programme**. To create a cybersecurity programme to provide regular workshops and training, clarifying for the team members the practices and procedures they must adopt in order to keep both themselves and the information safe;
5. **Security Routine**. The establishment of a security routine, addressed for the "Human Resources" system: request personnel identification for accessing the "Physical Systems" environment; adoption of security procedures; participation on cybersecurity training; respect to the security rules; and others.
6. **Information Technology**. To develop information technology solutions applied to avoid cybersecurity issues: backup plan; confidentiality of data; data separation; encryption/decryption mechanisms; firewall and antivirus; information control; install firewalls, antivirus protection; intrusion detection; proposing traditional distributed database technology; scheduling techniques; secure data access; secure sensitive data [5]. Besides, it is indicated the creation of a framework to identify cybersecurity risks, taking as examples the ones indicated within the studies of Mantha & Soto [3] and Yusta et al. [57]. Moreover, it is also indicated the creation and maintenance of two authorization and authentication processes to manage information within the CDE, based on the infrastructure presented at "Critical Infrastructure". The first process (step "1") grants the visualization and insertion of information. The second process (step "2") grants the necessity to edit/extract/exclude information. Here, the presented authorization and authentication processes are based on the studies of Manogaran et al. [5]. Figure 43 illustrates them:

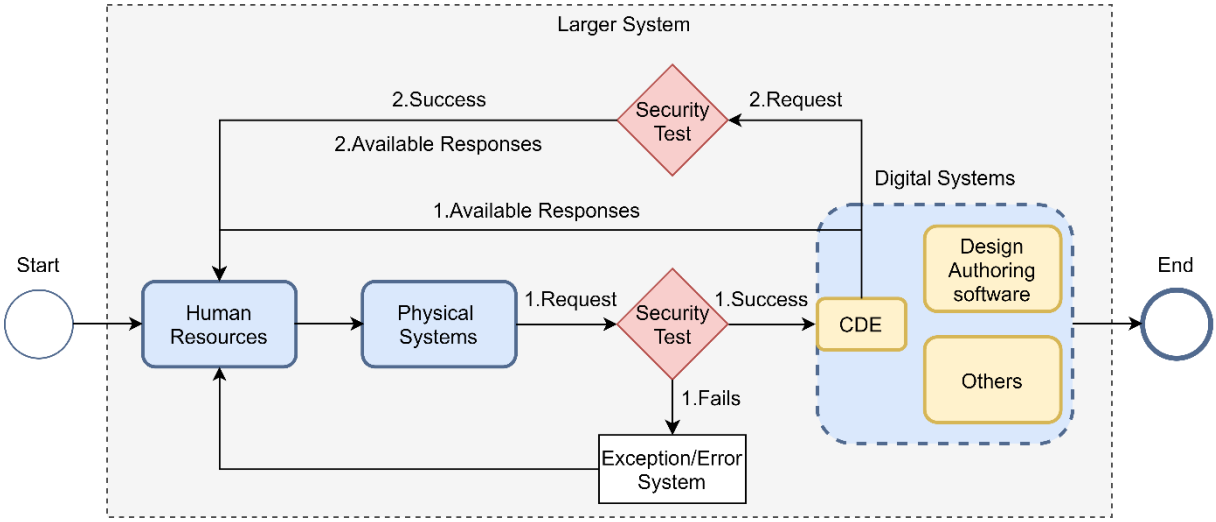

Figure 43: authorization and authentication processes. Source: the author.

7. **Communication and Exchange**. The establishment of enhanced communication protocols [5], assuring a secure channel of communication and exchange of information between the Client/Employer and the supplier and its supply chain;
8. **Resilience**. The establishment of resilience mechanisms applied for the entire infrastructure. The Cybersecurity Team shall focus within the cyber-resilience theme, considering potential causes of both human and cyber-physical disruptions, assuring that the leading systems and processes are maintained, and have available systems and processes that can detect and answer to disruptive events on time [41];
9. **Internal Audit Protocol**. The establishment of an internal audit protocol, which shall be an essential process to help the BIM Manager to assess the cybersecurity engagement of all the team members. Research questionnaires, combined with other audit tools, may be a powerful tool to make this assessment possible. The completion of the research questionnaires shall provide enough information for the Cybersecurity Team of the assessed organization take security measures in order to mitigate risks.

The next subsection presents information used to design the research questionnaires (see APPENDIX A) mentioned at the “Internal Audit Protocol” item.

6.3 Assessment on Cybersecurity

This subsection informs how the research questionnaires, developed to assess the cybersecurity engagement of the supplier and its supply chain responsible for the penal building project design process, were designed. The study entitled “Designing and using research questionnaires” developed by Rowley [65], is a basis for the designing of the questionnaires.

According to Rowley [65], the term “research questionnaire” refers to questionnaires that are used “as part of an academic research project.” He also mentions that the template of a questionnaire can present

a different series of open and closed questions usually used to be completed without interaction between the researcher and the questionnaire's respondents.

The author also mentions that questionnaires are used by researchers when they want to profile "the sample in terms of numbers (e.g. the proportion of the sample in different age groups) or to be able to count the frequency of occurrence of opinions, attitudes, experiences, processes, behaviours, or predictions." In this research study, the questionnaires were designed to count the frequency of occurrence of opinions, attitudes, experiences, processes and behaviours.

Further, Rowley [65] informs how the questions of a questionnaire can be formulated, differing from each other as "closed" and "open". In this study, it was used the closed questions to design the questionnaires, specifically the Likert scale (Figure 44) questions and the category ones (Figure 45). According to the author, with the Likert scale questions "respondents are asked to indicate how strongly they agree or disagree with a series of statements."

1. How innovative are we?

Please respond on the following scale.

In our organisation we...	Strongly Agree	Agree	Neither agree or disagree	Disagree	Strongly disagree
encourage new ideas throughout the organisation.					
encourage and support innovative employees.					
gather and use information about our trade customers.					
are effective at implementing change.					
gather and use information about our consumers/end-users.					
put innovation at the heart of our strategic planning.					
gather and use information about our competitors & markets.					
engage in shaping an innovative organisational culture.					

Figure 44: extract from a questionnaire on innovation orientation. Source: Rowley [65]**.**

Category question

How many times last week did you use our e-banking facilities? Please tick one response

Never		Once		2-3 times		4-5 times		5+times	

Figure 45: example of a closed question. Source: Rowley [65]**.**

The option for closed questions was made because they are of quick response and they "are easier to code and analyse, which is particularly important if the number of questionnaires collected is quite large" [65]. Furthermore, it was given special attention to the questions during the designing of the questionnaires, based on the Rowley's advice. According to him, the questions should be:

- are as short as possible;
- are not leading or have implicit assumptions;
- do not include two questions in one;
- only exceptionally invite "yes/no" answers;
- are not too vague or general; do not use double negatives;
- are not, in any sense, invasive, or asking questions that the respondent is unlikely to want to answer; and
- do not invite respondents to breach confidentiality.

Moreover, the organization of the questions was based on Rowley's advice [65], when he says that their order "should be clear, often with questions clustered under theme or section headings. Often earlier questions set the context for later questions." Besides, it was also considered the entire questionnaires' content organization, clarifying for the respondent their logical sequence. Rowley says that "The quality of the response will also be enhanced by a clear title, coupled with a good, short introductory paragraph at the beginning of the questionnaire" [65].

Therefore, once understood the strategies for designing research questionnaires, it is presented the research questionnaires developed for this study. The questionnaires were developed for three main targets:

a) a common team member;
b) the EIR Manager; and
c) the BEP Manager.

This division is made considering that each team member has a particular role and responsibility within the project design process. Besides, even if there is a BIM Manager, he/she not necessarily deals with both the BEP and EIR documents.

Furthermore, the research questionnaire respondent will be guided through the following structure:

1. *Presentation topic*. Presenting the questionnaire's authors, informing the research aim and explaining how the research is developed;
2. *Respondent's profile*. The respondent is invited to answer questions regarding his/her profile;
3. *Infrastructure*. The respondent is invited to answer questions based on three different "assets", mentioned in the "Critical Infrastructure" subsection: Human Resources, Physical Systems and Digital Systems.

7 CONCLUSIONS

This research has started the debate upon the current disruptive innovations within the AEC/FM industry. These disruptive innovations also enabled by BIM methodology and technology have also provided possibilities for the professionals of the sector to work collaboratively and interconnected. Besides, it also informs about Cybersecurity issues, exposing the fragility of Cyber-physical spaces, vulnerable to cyber-depend crimes. The recent Cybersecurity incidents at the Civil Construction sector is also presented, signalling it shall quickly implement Cybersecurity measures in order to overcome them.

Through the information presented in the "LITERATURE REVIEW" chapter, it is possible to realize the absence of robust information regarding sensitive assets. Besides, it is noticeable the scarcity of standards and protocols addressed to Cybersecurity, principally to the protection of the CDE of sensitive assets. In this sense, it is recommended that the International Organization for Standardization keeps deepening its studies regarding Cybersecurity measures.

Along with the literature investigation and the data collection presented in the "PENAL BUILDINGS" chapter, it is clear that the concept and the architectural model of penal buildings have evolved continuously during the centuries; and, unfortunately, the incarcerated population numbers have not decreased during the last decades. Moreover, the escape attempts have incited human creativity, producing many stories in which the inmates try to experience freedom again, reaching success in some cases. Furthermore, the criminal system expenditure is significant in some countries; and the values keep raising despite law enforcement measures and the improvement of social well-being.

Still, in the "SECURITY CHALLENGES" chapter, it is clear that the more interconnected the world gets, the higher is the tendency of the increasing on Cybercrime activities. Also, it is frightening to realize the effects that a global health crisis can have upon the Cyber-physical spaces, enhancing the Cyber-dependent crimes. Furthermore, the investigation upon the existing building practices infrastructure showed the complexity of the systems which enable the information flow. Moreover, the "CYBERSECURITY MEASURES" chapter shows that some professionals are researching, proposing and also developing Cybersecurity measures for some sectors; however, just a few contemplate the AEC/FM industry.

In the "ANALYSIS" chapter, it was demonstrated the risks involving the existing building practices infrastructure, mainly the one connected with the CDE. Besides, the "Cybersecurity Protocol" indicates a set of possibilities for the professionals of the AEC/FM sector to mitigate or avoid Cybersecurity issues. Here is highlighted the importance of establishing a "Cybersecurity Team", a team capable of gathering all the necessary information and indicating procedures that shall guide the company for Cybersecurity "good practices".

Moreover, it is vital that the Cybersecurity Team design a risk management strategy, enabling the identification, analysis, evaluation and controlling of risks. A risk management strategy can eliminate many possibilities of damages within the infrastructure and, in the worst case, avoid sensitive data loss and theft of intellectual property, for instance. The risk management strategy must be continuously updated according to the changes that may happen during the project design phase, with the purpose to assure its feasibility.

Furthermore, even considering the few standards and documents already available about Cybersecurity, the organization must establish some "Cybersecurity Documents", following the standard's contents. These documents can provide information on "good practices" that shall be introduced periodically. It is recommended that the introduction of "good practices" may happen through a "Cybersecurity Programme" when workshops and training are managed. The workshops may provide the possibility of information exchange among the supply chains according to their experiences. It is also recommended a "Security Routine" implementation for the success of the Cybersecurity Program. An established routine can make team members naturally incorporate good daily practices.

Also, "Information Technology" solutions are an essential part of any organization. The AEC/FM sector shall pay special attention to the installation of security tools like antivirus, firewalls, intrusion detection and others. The "Communication and Exchange" subjects are equally important in the Cybersecurity approach, mainly in these days when e-mails are not the unique communication tool available. The Covid-19 pandemic has changed the way people used to reunite, exposing the fragility of the online resources.

The "Resilience" subject arises from the imminent risks involving an organization infrastructure. An organization shall design resilience mechanisms to overcome Cybersecurity issues, assuring the continuity of the work under development.

Moreover, audit programmes are substantial to keep the organization aligned with the established goals and tasks. This way, the organization shall establish an "Internal Audit Protocol", which shall expose the non-compliances observed during the work development, enabling the team members to adjust their practices to meet the organization's goals.

Therefore, this research concludes that, despite the Cybersecurity issues inherent to this new digital era, the adoption of Cybersecurity procedures to protect the collaborative digital environment of a sensitive asset is still at its beginning. Besides, differently from what some authors have stated, the CDE vulnerabilities are directly related to the criticality of the whole infrastructure of the building design process, i.e. it embraces the "Human Sources", the "Physical" and the "Digital" systems. Thus, protecting the whole infrastructure is a way to assure protection for the CDE.

For future works, it is recommended the application of the research questionnaires developed for this study. Research questionnaires are a valuable tool to investigate the attitudes, opinions, experiences, processes, and others; they can provide an excellent approach to the current situation of the organization under analysis. It is also recommended the development and implementation of a “maturity model” to classify the organization Cybersecurity approach. The maturity models are useful to measure the effectiveness and the efficiency in which the organization is working.

8 REFERENCES

[1] L. Blanco, T. Dohrmann, J. P. Julien, J. Law, and R. Palter, "Governments can lead construction into the digital era," *McKinsey&Company*, no. April, pp. 1–8, 2019.

[2] K. Bartlett, J. L. Blanco, D. Rockhill, and G. Strube, "Breaking the mold: The construction players of the future," *Voices*, pp. 1–4, 2019.

[3] B. R. K. Mantha and B. G. de Soto, "Cyber security challenges and vulnerability assessment in the construction industry," no. August, pp. 29–37, 2019, doi: 10.3311/ccc2019-005.

[4] R. Waugh, "Is cybersecurity keeping up with the internet of things?," *The Telegraph*, no. January 2018, Jan-2018.

[5] Springer, *Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing*. Cham: Springer Nature, 2017.

[6] Europol, "Internet Organised Crime Threat Assessment (IOCTA)," 2019.

[7] A. Hammi and A. Bouras, "Towards Safe-Bim Curricula Based on the Integration of Cybersecurity and Blockchains Features," *INTED2018 Proc.*, vol. 1, pp. 2380–2388, 2018, doi: 10.21125/inted.2018.0453.

[8] B. G. de Soto, A. Georgescu, B. Mantha, Ž. Turk, and A. Maciel, "Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan," vol. 0, no. May, pp. 1–20, 2020, doi: 10.20944/PREPRINTS202005.0213.V1.

[9] The British Standards Institution, "PAS 1192-5. Specification for security-minded building information modelling, digital built environments and smart asset management," *BSI Standards Limited*. United Kingdom, 2015.

[10] ISO 19650-1, "Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles," vol. 1. Geneva, 2018.

[11] E. A. Pärn and D. Edwards, "Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence," *Eng. Constr. Archit. Manag.*, vol. 26, no. 2, pp. 245–266, 2019, doi: 10.1108/ECAM-03-2018-0101.

[12] Y. Arayici, C. Egbu, and P. Coates, "BUILDING INFORMATION MODELLING (BIM) IMPLEMENTATION AND REMOTE CONSTRUCTION PROJECTS: ISSUES,

CHALLENGES, AND CRITIQUES," *J. Inf. Technol. Constr.*, vol. 17, p. 19, 2012, doi: 10.1714/641.7477 LK - http://sfx.library.uu.nl/utrecht?sid=EMBASE&issn=18276806&id=doi:10.1714%2F641.7477&atitle=RVOT+obstruction+and+right+bundle+branch+block+in+hypertrophic+cardiomyopathy%3A+A+case+report&stitle=G.+Ital.+Cardiol.&title=Giornale+Italiano+di+Cardiologia&volume=12&issue=5&spage=161S&epage=&aulast=Parato&aufirst=Vito+Maurizio&auinit=V.M.&aufull=Parato+V.M.&coden=&isbn=&pages=161S-&date=2011&auinit1=V&auinitm=M.

[13] The British Standards Institution, "PAS 1192-2. Specification for information management for the capital/delivery phase of construction projects using building information modelling," no. 1. 2013.

[14] The Computer Integrated Construction Research Group, "Building Information Modeling Execution Planning Guide," *The Pennsylvania State University*, vol. 53. p. 160, 2010, doi: 10.1017/CBO9781107415324.004.

[15] C. Castaing *et al.*, "BIM and ISO 19650 from a project management perspective." .

[16] The British Standards Institution, *Little Book of BIM*. 2019.

[17] W. Abdelhameed and W. Saputra, "Integration of building service systems in architectural design," *J. Inf. Technol. Constr.*, vol. 25, pp. 109–122, 2020, doi: 10.36680/j.itcon.2020.007.

[18] A. Bradley, H. Li, R. Lark, and S. Dunn, "BIM for infrastructure: An overall review and constructor perspective," *Autom. Constr.*, vol. 71, pp. 139–152, 2016, doi: 10.1016/j.autcon.2016.08.019.

[19] E. C. W. Lou and M. Alshawi, "Critical success factors for e-tendering Implementation in construction collaborative environments: people and process issues," *Electron. J. Inf. Technol. Constr.*, vol. 14, no. May, pp. 98–109, 2009.

[20] S. Mordue, "Implementation of a Common Data Environment: The Benefits, Challenges & Considerations," no. August. Edinburgh, p. 32, 2018.

[21] H. Boyes, "Building Information Modelling (BIM): Addressing the cyber security issues," London, 2014.

[22] H. A. Boyes, "Cyber security of intelligent buildings: A review," *IET Conf. Publ.*, vol. 2013, no. 620 CP, 2013, doi: 10.1049/cp.2013.1698.

[23] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, pp. 13–21, 2014, doi: 10.22215/timreview835.

[24] M. Barrett, “Framework for improving critical infrastructure cybersecurity,” *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.

[25] M. Foucault, *Discipline and Punish: The Birth of the Prison*, vol. 68, no. 3. 1995.

[26] P. Steadman, “The Contradictions of Jeremy Bentham’s Panopticon Penitentiary,” *J. Bentham Stud.*, no. January 2007, 2007, doi: 10.14324/111.2045-757x.030.

[27] S. Henley, “The 21st century model prison,” *Proceedings. 4th Int. Sp. Syntax Symp. London*, no. Figure 1, 2003.

[28] R. Muir and I. Loader, “Tomorrow’ s Prisons : Designing the future prison estate,” no. April, 2010.

[29] R. Garside *et al.*, “The Future of Prisons,” *Prison Serv. J.*, vol. 231, no. May, pp. 22–30, 2017.

[30] C. Weller, “Dutch prisons are closing because the country is so safe,” *Independent*, no. May 2017, pp. 1–9, May-2017.

[31] G. Alessi, “Decapitations and butchery, as Brazilian jail riot leaves at least 50 dead,” *El País*, São Paulo, pp. 1–6, 2017.

[32] G. Stargardter, “Bolsonaro targets deadly gangs run from Brazil’s prisons,” *Reuters*, Porto Alegre, pp. 1–14, Apr-2019.

[33] C. (University of C. Haney, “The Psychological Impact of Incarceration: Implicatons for Post-Prison Adjustment,” *U.S. Dep. Heal. Hum. Serv.*, pp. 1–18, 2001.

[34] G. Farrell and K. Clark, “WHAT DOES THE WORLD SPEND ON CRIMINAL JUSTICE?,” *Comp. Sociol.*, vol. 20, no. 1–2, 2004, doi: 10.1177/002071520104200103.

[35] The Inter-American Development Bank, “The costs of crime and violence: new evidence and insights in Latin America and the Caribbean,” *Inter-American Development Bank*. Washington, D.C. 20577, p. 12, 2017.

[36] M. J. F. Silva, F. Salvado, P. Couto, and Á. V. e Azevedo, “Roadmap Proposal for Implementing Building Information Modelling (BIM) in Portugal,” *Open J. Civ. Eng.*, vol. 06, no. 03, pp. 475–481, 2016, doi: 10.4236/ojce.2016.63040.

[37] S.-G. BRASIL, *Decreto nº 10.306*. Brasil: Subchefia para Assuntos Jurídicos, 2020, pp. 1–5.

[38] V. Mavroeidis and S. Bromander, “Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence,” *Proc. - 2017*

Eur. Intell. Secur. Informatics Conf. EISIC 2017, vol. 2017-Janua, pp. 91–98, 2017, doi: 10.1109/EISIC.2017.20.

[39] K. Nakata, "Global Threat Intelligence Report," 2019.

[40] J. Marks and T. Riley, "The Cybersecurity 202 : Coronavirus pandemic unleashes unprecedented number of online scams," *The Washington Post*, 2020.

[41] H. Boyes, "Resilience and Cyber Security of Technology in the Built Environment," London, United Kingdom, 2013.

[42] J. Swaine, "New US charges against Julian Assange could spell decades behind bars," *The Guardian*, New York, pp. 1–6, May-2019.

[43] G. Greenwald, E. MacAskill, and L. Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations," *The Guardian*, Hong Kong, p. 1, Jun-2013.

[44] G. C. Wilshusen, "Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies," *GAO Highlights*. 2015.

[45] Intel Information Technology, "Threat Agent Library Helps Identify Information Security Risks," no. September. 2007.

[46] The U.K. National Cyber Security Centre, "Common Cyber Attacks: Reducing the Impact," *UK Government*, no. January. p. 17, 2016.

[47] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide Recommendations," *NIST Special Publication*. p. 79, 2012, doi: 10.6028/NIST.SP.800-61r2.

[48] Royal Institute of British Architects - RIBA, "RIBA Plan of Work 2020," London, 2020.

[49] Tribunal de Contas da União, "Obras Públicas: Recomendações Básicas para a Contratação e Fiscalização de Obras de Edificações Públicas," *Tribunal de Contas da União*. pp. 429–432, 20184, doi: 10.2307/j.ctv3dnqx4.13.

[50] ISO 19650-2, "Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 2: Delivery phase of the assets," vol. 1. Geneva, 2018.

[51] Y. Z. Lun, A. D'Innocenzo, I. Malavolta, and M. D. Di Benedetto, "Cyber-Physical Systems Security: a Systematic Mapping Study," pp. 1–32, 2016, doi: 10.1016/j.jss.2018.12.006.

[52] J. Moteff, C. Copeland, J. Fischer, I. Ave, and S. E. Washington, "What Makes an Infrastructure Critical?," Washington, D.C., 2003.

[53] R. L. Church, M. P. Scaparra, and R. S. Middleton, "Identifying critical infrastructure: The median and covering facility interdiction problems," *Ann. Assoc. Am. Geogr.*, vol. 94, no. 3, pp. 491–502, 2004, doi: 10.1111/j.1467-8306.2004.00410.x.

[54] A. T. Murray, T. C. Matisziw, and T. H. Grubesic, "Critical network infrastructure analysis: Interdiction and system flow," *J. Geogr. Syst.*, vol. 9, no. 2, pp. 103–117, 2007, doi: 10.1007/s10109-006-0039-4.

[55] M. J. Egan, "Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems," *J. Contingencies Cris. Manag.*, vol. 15, no. 1, pp. 4–17, 2007, doi: 10.1111/j.1468-5973.2007.00500.x.

[56] C. Aradau, "Security that matters: Critical infrastructure and objects of protection," *Secur. Dialogue*, vol. 41, no. 5, pp. 491–514, 2010, doi: 10.1177/0967010610382687.

[57] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, vol. 39, no. 10, pp. 6100–6119, 2011, doi: 10.1016/j.enpol.2011.07.010.

[58] A. Jerraya *et al.*, "Hardware/software co-design," *Des. Syst. a Chip Des. Test*, vol. 85, no. 3, pp. 133–158, 1997, doi: 10.1007/0-387-32500-X_7.

[59] The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," 2018.

[60] M. Guri, "AiR-ViBeR: Exfiltrating Data from Air-Gapped Computers via Covert Surface ViBrAtIoNs." Cyber-Security Research Center, pp. 1–12, 2020.

[61] UK Government, "10 Steps to Cyber Security." The U.K. National Cyber Security Centre, p. 1, 2012.

[62] C. McPhee and O. Khan, "Editorial: Cyber- Resilience in Supply Chains," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, pp. 33–39, 2014.

[63] H. Boyes, "Cybersecurity and Cyber-Resilient Supply Chains," *Technol. Innov. Manag. Rev.*, vol. 5, no. 4, pp. 28–34, 2015, doi: 10.22215/timreview888.

[64] Government of Canada, "Criminal Code," *Minister of Justice*, vol. C–46. Minister of Justice, p. 1131p., 1985.

[65] J. Rowley, "Designing and using research questionnaires," *Manag. Res. Rev.*, vol. 37, no. 3, pp. 308–330, 2014, doi: 10.1108/MRR-02-2013-0027.

[1] Guid, N., Strnad, D. 2015. Umetna inteligenca. Maribor, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

[2] Analytica Wiki. 2019. Optimization Characteristics. http://wiki.analytica.com/Optimization_Characteristics (Pridobljeno 26. 08. 2019).

[3] Autodesk. 2019. Insight. https://www.autodesk.com/products/insight/overview (Pridobljeno 28. 08. 2019).

[4] Autodesk. 2019. Revit Features. https://www.autodesk.com/products/revit/features (Pridobljeno 22. 08. 2019).

[5] DesignTech. 2019. Parametric Modelling. https://www.designtechsys.com/articles/parametric-modelling (Pridobljeno 28. 08. 2019).

[6] Dynamo Primer. 2019. What is Dynamo. https://primer.dynamobim.org/01_Introduction/1-2_what_is_dynamo.html (Pridobljeno 22. 08. 2019).

[7] Dynamo Primer. 2019. What is Visual Programming. https://primer.dynamobim.org/01_Introduction/1-1_what_is_visual_programming.html (Pridobljeno 26. 08. 2019).

[8] Ladybug Tools. 2019. Tools. https://www.ladybug.tools/index.html (Pridobljeno 28. 08. 2019).

[9] Nagy, D. 2017. Introduction to computational design. https://medium.com/generative-design/introduction-to-computational-design-6c0fdfb3f1 (Pridobljeno 14. 08. 2019).

[10] PBL Lab Stanford. 2019. Team Pacific Spring Presentation. http://pbl.stanford.edu/AEC%20projects/Year%202018-2019/Spring/Pacific-Spring2019.pdf (Pridobljeno 12. 08. 2019).

[11] Refinery Primer. 2019. Solvers. https://refineryprimer.dynamobim.org/05-algorithms/05-04_solvers (Pridobljeno 13. 08. 2019).

[12] Refinery Primer. 2019. What is Generative Design. https://refineryprimer.dynamobim.org/01-introduction/01-02_what-is-generative-design (Pridobljeno 18. 08. 2019).

[13] Refinery Primer. 2019. What is Refinery. https://refineryprimer.dynamobim.org/01-introduction/01-09_what-is-refinery (Pridobljeno 21. 08. 2019).

[14] Stasiuk, D. 2018. Design Modeling Terminology. https://archinate.files.wordpress.com/2018/06/dstasiuk-design-modeling-terminology1.pdf (Pridobljeno 29. 07. 2019).

9 APPENDIX A

9.1 General Questionnaire

Dear participant, the present questionnaire makes part of a master thesis research, that has been developed by Vítor Ferronato de Lira, on his BIM A+ master course at the University of Ljubljana, tutored by Professor dr Žiga Turk, from the same university. The answers for the questions presented in this survey will contribute with the researcher's apprehension upon the workgroup team members' **cybersecurity engagement** regarding the design process of sensitive assets, here understood as penal buildings.

The questionnaire is developed through the following steps: first, it is traced the team member profile; next is assessed the vulnerabilities of the project design infrastructure, divided into three categories: Human Resources, Physical Systems and Digital Systems.

Note: for security reasons, the questionnaire was developed to be answered **anonymously**.

9.1.1 Team Member Profile

How old are you?

a) Under 20
b) Between 20 – 25
c) Between 25 – 35
d) Between 35 – 45
e) Over 45

In each of the following professional areas…	Architecture and Urbanism	MEP Engineering	Civil Engineering	Land Survey	Other
do you have your bachelor's degree?	□	□	□	□	□
are you participating of within the penal buildings project?	□	□	□	□	□

I have been…	Less than six months	More than six months	One year	For years
working within the Civil Construction industry?	□	□	□	□
working within the BIM methodology?	□	□	□	□
working within this penal buildings project design?	□	□	□	□

9.1.2 Human Resources

The Human Resources are one of the most critical assets of a project design infrastructure. The team members, participants of the design project, detain roles and responsibilities that, aligned with their hard and soft skills, deliver the products required by the Client/Employer. However, as vital assets for the project design development, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

I consider that...	Fully agree	Agree	Neutral	Disagree	Strongly disagree
I should be more acquainted with the cybersecurity theme.	□	□	□	□	□
I should be more aware of cybersecurity risks.	□	□	□	□	□
I should have participated in a cybersecurity workshop/training.	□	□	□	□	□
some manual/guide about cybersecurity should have been introduced to me.	□	□	□	□	□
I could be vulnerable to: assaults, bodily harm and acts and omissions causing danger to the person, defamatory libel and/or extortion due to your participation in the penal buildings project.	□	□	□	□	□
I could be vulnerable to: fake news, hate propaganda, homicide, interception of communications and/or kidnapping, trafficking in persons, hostage taking and abduction, while participating in the penal buildings project.	□	□	□	□	□
I could be vulnerable to: loss or disclosure of commercially sensitive information, loss or disclosure of intellectual property, murder, manslaughter and/or release of personally identifiable information, while participating in the penal buildings project.	□	□	□	□	□
I could not be vulnerable to any kind of human risk while participating in the penal buildings project.	□	□	□	□	□

9.1.3 Physical Systems

Physical Systems are understood in this survey as hardware and physical spaces supportive for the development of the Human Resources activities. They are also considered as assets because they play a vital role in the project design development and their absence can compromise the schedule for the

deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

Personally, I…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
use more my personal devices than the ones from my job.	□	□	□	□	□
use more the devices from my job.	□	□	□	□	□
access the internet from the desktop computer and/or the laptop.	□	□	□	□	□
access the internet from the smart phone and/or smart watch.	□	□	□	□	□
access the internet from the tablet.	□	□	□	□	□
have already had some device hacked.	□	□	□	□	□
have already had the desktop computer and/or the laptop hacked.	□	□	□	□	□
have already had the smart phone and/or smart watch hacked.	□	□	□	□	□
have already had the tablet hacked.	□	□	□	□	□
have already been a victim of attrition, external/removable media and/or loss of theft of equipment, while participating in the penal buildings project.	□	□	□	□	□
have already been a victim of sabotage and/or system failure, while participating in the penal buildings project.	□	□	□	□	□

9.1.4 Digital Systems

Digital Systems are understood in this survey as software supportive for the development of the Human Resources activities within the Physical Systems. They are also considered as assets, because they play a vital role for the project design development and their absence can compromise the schedule for the deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

Personally, I…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
am used to access the Internet form a domestic network.	□	□	□	□	□
am used to access the Internet form a public network.	□	□	□	□	□
use the same password for all of my logins.	□	□	□	□	□

am used to logout from my e-mail accounts after finishing my goals.	□	□	□	□	□
know what is a Common Data Environment (CDE) - (ISO 19650-1, 2018).	□	□	□	□	□
do consider that I had a satisfactorily presentation of the CDE "good practices".	□	□	□	□	□
do not share my CDE password with others.	□	□	□	□	□
access the CDE more than once a day.	□	□	□	□	□
access the CDE more than once a week.	□	□	□	□	□
access the CDE just once of a month.	□	□	□	□	□
do believe to have access to all the CDE stored information.	□	□	□	□	□
am used to logout from the system after using the CDE.	□	□	□	□	□
am aware of: malware, ransomware and/or virus.	□	□	□	□	□
am aware of: cyber threats and/or cyber-attacks.	□	□	□	□	□
am aware of: sensitive asset, sensitive data and/or sensitive information.	□	□	□	□	□
have already been a victim of the following cyber-attacks: blackmail, fingerprinting, input capture and/or phishing/spear phishing.	□	□	□	□	□
have already been a victim of the following cyber-attacks: scanning, social engineering, spamming and/or spoofing.	□	□	□	□	□
have never been a victim of cyber-attacks.	□	□	□	□	□

9.2 EIR Manager Questionnaire

Dear participant, the present questionnaire makes part of a master thesis research, that has been developed by Vítor Ferronato de Lira, on his BIM A+ master course at the University of Ljubljana, tutored by Professor dr. Žiga Turk, from the same university. The answers for the questions presented in this survey will contribute with the researcher's apprehension upon the workgroup team members' **cybersecurity engagement** regarding the design process of sensitive assets, here understood as penal buildings.

You have received this questionnaire because you are the responsible for the elaboration and/or management of Exchange Information Requirements – EIR - [10] document.

The questionnaire is developed through the following steps: first, it is traced the Profile of the EIR Manager; next is assessed the vulnerabilities of the project design infrastructure, divided into three categories: Human Resources, Physical Systems and Digital Systems.

Note: for security reasons, the questionnaire was developed to be answered **anonymously**.

9.2.1 Profile of the EIR Manager

How old are you?

f) Under 20
g) Between 20 – 25
h) Between 25 – 35
i) Between 35 – 45
j) Over 45

What is your bachelor's degree?

- □ Architect and Urbanist
- □ Electrical Engineer
- □ Mechanical Engineer
- □ Plumbing Engineer
- □ Civil Engineer
- □ Land Surveyor
- □ Other: _____

I have been…	Less than 5	Between 20 – 25	Between 25 – 35	Between 35 – 45	More than 45
working within the Civil Construction industry for:	□	□	□	□	□
working within the BIM methodology for:	□	□	□	□	□

9.2.2 Human Resources

The Human Resources are one of the most important assets of a project design infrastructure. The team members, participants of the design project detain roles and responsibilities that, aligned with their hard and soft skills, deliver the products required by the Client/Employer. However, as vital assets for the project design development, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

The Client/Employer…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
requested the elaboration of any cybersecurity manual/guide.	□	□	□	□	□
requested some risk assessment of the work practices during the project design development process.	□	□	□	□	□
request some cybersecurity workshop/training certificate from my company.	□	□	□	□	□
requested some human-risk mitigation measures from my company.	□	□	□	□	□

9.2.3 Physical Systems

Physical Systems are understood in this survey as hardware and physical spaces supportive for the development of the Human Resources activities. They are also considered as assets because they play a vital role in the project design development and their absence can compromise the schedule for the deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

The Client/Employer…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
allows the access of my company's personnel to his/her headquarter building.	□	□	□	□	□
has lent equipment for my company.	□	□	□	□	□
has borrowed equipment from my company.	□	□	□	□	□
requested some cybersecurity physical-risk mitigation measures from my company.	□	□	□	□	□

9.2.4 Digital Systems

Digital Systems are understood in this survey as software supportive for the development of the Human Resources activities within the Physical Systems. They are also considered as assets, because they play a vital role in the project design development and their absence can compromise the schedule for the deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

The Client/Employer…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
has established the official means of communication (e-mail, applications, etc.) with my company.	□	□	□	□	□
has established that the Common Data Environment (CDE) (ISO 19650-1, 2018) should to be an application (Tonido, etc.).	□	□	□	□	□
has established that the Common Data Environment (CDE) (ISO 19650-1, 2018) should to be an Internet-based platform.	□	□	□	□	□
access the CDE once a month.	□	□	□	□	□
access the CDE twice a month.	□	□	□	□	□
access the CDE more than three times a month.	□	□	□	□	□
has limited access to the CDE.	□	□	□	□	□
has unlimited access to the CDE.	□	□	□	□	□
does not have access to the CDE.	□	□	□	□	□
has established the size of the CDE.	□	□	□	□	□
has established the CDE management.	□	□	□	□	□
requested some cybersecurity digital-risk mitigation measures.	□	□	□	□	□

9.3 BEP Manager Questionnaire

Dear participant, the present questionnaire makes part of a master thesis research, that has been developed by Vítor Ferronato de Lira, on his BIM A+ master course at the University of Ljubljana, tutored by Professor dr. Žiga Turk, from the same university. The answers for the questions presented in this survey will contribute with the researcher's apprehension upon the workgroup team members' **cybersecurity engagement** regarding the design process of sensitive assets, here understood as penal buildings.

You have received this questionnaire because you are the responsible for the elaboration and/or management of BIM Execution Plan – BEP - [50] document.

The questionnaire is developed through the following steps: first, it is traced the Profile of the BEP Manager; next is assessed the vulnerabilities of the project design infrastructure, divided into three categories: Human Resources, Physical Systems and Digital Systems.

Note: for security reasons, the questionnaire was developed to be answered **anonymously**.

9.3.1 Profile of the BEP Manager

How old are you?

k) Under 20
l) Between 20 – 25
m) Between 25 – 35
n) Between 35 – 45
o) Over 45

What is your bachelor's degree?

□ Architect and Urbanist
□ Electrical Engineer
□ Mechanical Engineer
□ Plumbing Engineer
□ Civil Engineer
□ Land Surveyor
□ Other: _____

I have been…	Less than 5	Between 20 – 25	Between 25 – 35	Between 35 – 45	More than 45
working within the Civil Construction industry for:	□	□	□	□	□
working within the BIM methodology for:	□	□	□	□	□

9.3.2 Human Resources

The Human Resources are one of the most important assets of a project design infrastructure. The team members, participants of the design project detain roles and responsibilities that, aligned with their hard and soft skills, deliver the products required by the Client/Employer. However, as vital assets in the project design development, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

It...	Fully agree	Agree	Neutral	Disagree	Strongly disagree
was elaborated some cybersecurity manual/guide to be implemented by the team members.	□	□	□	□	□
has been doing some risk assessment of the work practices during the project design development process.	□	□	□	□	□

was provided some cybersecurity workshop/training for the project design team members.	□	□	□	□	□
was established some human-risk mitigation measures.	□	□	□	□	□
has continuously been implemented risk assessment practices during the project design development.	□	□	□	□	□

9.3.3 Physical Systems

Physical Systems are understood in this survey as hardware and physical spaces supportive for the development of the Human Resources activities. They are also considered as assets, because they play a vital role in the project design development and their absence can compromise the schedule for the deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

It...	Fully agree	Agree	Neutral	Disagree	Strongly disagree
was established some cybersecurity physical-risk mitigation measures.	□	□	□	□	□
was established some equipment control.	□	□	□	□	□
was confirmed that all the equipment have a “warranty certificate”.	□	□	□	□	□
is allowed to borrow the physical equipment used to the project design development.	□	□	□	□	□
was established some “restriction access control” for the physical environment where are placed all the equipment supportive for the project development.	□	□	□	□	□
is required from the team members to use and present their personal identification when accessing the physical environment supportive for the project design development.	□	□	□	□	□
was established some entrance control at the physical environment supportive for the project design development.	□	□	□	□	□

9.3.4 Digital Systems

Digital Systems are understood in this survey as software supportive for the development of the Human Resources activities within the Physical Systems. They are also considered as assets, because they play a vital role in the project design development and their absence can compromise the schedule for the deliverable of the required products. Besides, they may be vulnerable to diverse threats. Considering the vulnerabilities of this referred asset, evaluate the questions below:

It…	Fully agree	Agree	Neutral	Disagree	Strongly disagree
was established that the Common Data Environment (CDE) - (ISO 19650-1, 2018) - is a local application (Tonido, etc.).	□	□	□	□	□
was established that the Common Data Environment (CDE) - (ISO 19650-1, 2018) - is an Internet-based platform.	□	□	□	□	□
was established the size of the CDE.	□	□	□	□	□
was established that CDE organization (work in progress, shared, published, archive) is the same as defined by the ISO 19650-1 (2018).	□	□	□	□	□
was established that all the team members of the project design group have access to the CDE.	□	□	□	□	□
was established some precaution against the access of dismissed personnel to the CDE.	□	□	□	□	□
was established some cybersecurity digital-risk mitigation measures.	□	□	□	□	□
was established some protection measures against cyber-attacks.	□	□	□	□	□
was established some information control procedure.	□	□	□	□	□