...::KENT AKADEMİSİ | URBAN ACADEMY

Volume: 18 Issue: 5 - 2025 | Cilt: 18 Sayı 5 - 2025

ARTICLE INFO | MAKALE KÜNYESİ

Article Type: Research Article | Araştırma Makalesi
Submission Date | Gönderilme Tarihi: 28.02.2025
Admission Date | Kabul Tarihi: 13.07.2025

CITATION INFO | ATIF KÜNYESİ

Güç, A. and Bülbül Bahtiyar, T. (2025). An Evaluation of the Adoption of Cybersecurity Culture in Architectural Education, *Kent Akademisi Dergisi*, *18*(5):2883-2898. https://doi.org/10.35674/kent.1648488

An Evaluation of the Adoption of Cybersecurity Culture in Architectural Education

Mimarlık Eğitiminde Siber Güvenlik Kültürünün Benimsenmesi Üzerine Bir Değerlendirme

Abdullah GÜÇ[1], Tuba BÜLBÜL BAHTİYAR[2]

ÖZ

Teknolojinin hızla ilerlemesi, diğer pek çok alanı olduğu gibi mimarlık alanını da dönüştürerek, giderek daha fazla birbirine bağlı ve dijital sistemlere dayanan yeni bir "akıllı yapılar" çağını başlatmıştır. Ancak Ortak ağa bağlanan ve birbirleriyle iletişim kurabilen nesneler ve cihazlar, potansiyel olarak siber saldırganların istismar edebileceği zayıflıklara ve açıklıklara sahip olup internete bağlı her türlü yapı, sistem ve donanım hacklenme riski ile karşı karşıyadır. Dolayısıyla bu kapsama giren her tür nesneyi ve yapıları geliştiren ve bunlarla ilgilenen uzmanlık dalının, profesyonel alanlarının bir parçası olacak şekilde "siber güvenlik kültürü"nü benimsemesi son derece önemlidir. Mimari tasarımda akıllı yapılara olan bağımlılık giderek artmasına rağmen siber güvenlik alanı mimarlık alanı içerisinde oldukça kısıtlı bir düzeyde ele alınmaktadır. Mimari tasarımlar, hiç durmadan farklılaşan siber tehditlere karşı ne kadar hazırlıklı planlanmaktadır sorusu ise bu çalışmanın temel problemini oluşturmaktadır. Siber güvenlik kültürü kavramıyla, siber tehditlerden korunma konusunda güçlü bir bilinç düzeyinin oluşturulması, kurumsal ve bireysel düzeyde ortak değerlerin ve normların oluşturulması, paylaşılması ve bu konudaki eylemlerin sürdürülebilir olması kastedilmektedir. Çalışma kapsamında "siber güvenlik kültürü"nün mimarlık alanındaki önemine değinilmesinin ardından bu kavramın mimarlık eğitim sistemine ne ölçüde adapte edildiği, dünyanın farklı ülkelerinde yer alan ve mimarlık bölümleriyle öne çıkan üniversitelerde kullanılan müfredat ve ders içerikleri incelenerek analiz edilmiştir. Araştırma sonucunda mevcut mimarlık eğitimi ve müfredatının yeni mezun bir mimarın kapsamlı bir siber güvenlik kültürü geliştirmesini sağlayacak bir yapıda henüz olmadığı çıkarımında bulunulmuştur.

Anahtar Kelimeler: Akıllı Bina, Mimarlık, Mimarlık Eğitimi, Siber Güvenlik, Siber Güvenlik Kültürü

ABSTRACT

The rapid advancement of technology has transformed the field of architecture (as in many other fields), ushering in a new era of "smart" buildings that are increasingly interconnected and reliant on digital systems. However, objects and devices that are connected to the common network and can communicate with each other have weaknesses and vulnerabilities that can potentially be exploited by cyber attackers, and all kinds of structures, systems and hardware connected to the internet are at risk of being hacked. Despite the increasing reliance on smart structures in architectural design, the field of cybersecurity is addressed at a very limited level within the field of architecture. The question of how prepared architectural designs are planned against ever-evolving cyber threats constitutes the main problem of this study. The concept of cyber security culture refers to the creation of a strong level of awareness about protection from cyber threats, the creation and sharing of common values and norms at the institutional and individual level, and the sustainability of actions in this regard. Within the scope of the study, after mentioning the importance of "cyber security culture" in the field of architecture, the extent to which this concept has been adapted to the architectural education system has been analyzed by examining the curricula and course contents used in universities in different countries of the world that stand out with their architecture departments. As a result of the research, it was concluded that the current architectural education and curriculum is not yet in a structure that will enable a newly graduated architect to develop a comprehensive cyber security culture.

Keywords: Architecture, Architectural Education, Cybersecurity, Cybersecurity Culture, Smart Building

[1] **Corresponding Author:** Sakarya University, abdullah.guc@ogr.sakarya.edu.tr, ORCID: 0000-0002-2540-5827

[2] Necmettin Erbakan University, tubabulbulbahtiyar@gmail.com, ORCID: 0000-0001-5204-8338

INTRODUCTION

Technological advancements have led to the development and usage of increasingly "smart" tools and objects that are becoming more interconnected through common networks. While the Internet was a network where predominantly computers (and people) communicated and interacted with each other until the early years of 2000s, it has evolved into the Internet of Things since the 2010s through the increased interconnectivity of an ever-growing number of objects and devices. Since the number of objects that are potential candidates to get “online” is much higher than the number of computers being manufactured, it is reasonable to assume that the number of connected objects will significantly exceed the number of computers and people. According to recent reports, approximately 18 billion objects were connected to the Internet as of 2024, and projections indicate this number is expected to double by 2030 (Statistica, 2024).

Any object or device that is connected to a network and communicates with other devices most likely has weaknesses and vulnerabilities that can potentially be exploited by cyber attackers and is at risk of being hacked. Therefore, it is extremely important that the professionals that develop and deal with such objects and buildings adopt a “cybersecurity culture” as part of their professional work.

Cybersecurity can be defined as the organization and aggregation of resources, processes and structures used to protect the public network and network-enabled systems and structures from unauthorized violations of legal (de jure) and de facto rights (Craigen et al., 2014). The cybersecurity approach first and foremost takes a proactive approach to protect valuable assets. For that purpose, it develops and utilizes various tools, policies, security measures, guidelines, risk management approaches, action plans and training (ITU, 2008).

The literature doesn’t provide us with an agreed upon definition for the concept of cybersecurity culture. The concept has been considered as a subculture of organizational culture in some studies (Uchendu et al., 2021), which defines it as a subculture that encompasses the attitudes, beliefs, values and knowledge that individuals use when interacting with the systems in an organization and carrying out related procedures, daily tasks and activities. In another study, cybersecurity culture is described in multiple layers, which are artifacts (policies, procedures, technologies, and physical security measures), behaviors (observable cybersecurity-related actions and practices of individuals and groups, including compliance with policies, incident reporting, and general security awareness), values and assumptions (core beliefs, principles, and shared understandings that shape cybersecurity behaviors and attitudes within the organization) (Reegård et al., 2019).

The concept of cybersecurity culture can be defined as the creation of a strong level of awareness about protection from cyber threats, the creation and sharing of common values and norms at the organizational and individual level, and the sustainability of actions in that regard.

As a holistic concept, cybersecurity culture emphasizes the importance of human factors in shaping an organization's overall approach to cybersecurity, going beyond the technical measures that would traditionally first come to mind and remain within the purview of IT officers. Developing a strong cybersecurity culture in any field or organization requires a multidisciplinary approach that integrates perspectives from various fields, including engineering, social sciences, architecture, and security studies (Craigen et al., 2014).

1. Methodology

A comprehensive literature review was carried out on cybersecurity education and architectural education and the intersection of the two. Recent studies highlight the growing importance of interdisciplinary approaches in cybersecurity education and various other fields. Interdisciplinary cybersecurity education fosters critical thinking, broader perspectives, and better communication skills (Lawrence-Fowler, 2013). It also helps students understand security behaviors across technical and non-technical fields (Jacob et al., 2019). In architectural education, interdisciplinary approaches are crucial for addressing complex urban issues and economic, social, and ecological crises (Kostešić & Jukić, 2024). Embedding cybersecurity awareness into design education has shown positive results, with students demonstrating increased consideration of cybersecurity aspects throughout the design process (Kim et al., 2019). However, maintaining this awareness over time remains a challenge. These studies indicate the need for holistic, collaborative educational models that prepare future professionals to navigate the complexities of cybersecurity in an increasingly interconnected world.

The literature review revealed that although cybersecurity is a growing concern in many fields, its integration into architecture curricula—particularly in the context of smart buildings, digital design tools, and interconnected environments—is still limited and largely underexplored. While existing studies discuss the need to reform architectural education in general (Taneja et al., 2024; Hollander et al., 2018; Pak & Verbeke, 2012), or address cybersecurity considerations in architectural design and practice (Boyes, 2013), (Ciholas et al., 2019), (Mylrea et al., 2017), there appears to be a clear gap in the literature when it comes to integrating cybersecurity as a formal component of architectural education.

These findings led to the formulation of the following sub-research questions:

1. Why is cybersecurity (culture) important for the field of architecture?
2. Have cybersecurity-related topics been incorporated into architectural education in universities?

In today’s context—where architecture and construction are increasingly intertwined with smart systems, IoT technologies, and digital tools—it becomes clear that cybersecurity is no longer just an IT concern. Architects play a growing role in shaping environments that are not only physically secure but also digitally resilient. Therefore, the presence or absence of cybersecurity awareness and training in architectural education has significant implications for how safe, functional, and future-ready our built environments will be.

Recognizing the importance of cybersecurity for the architectural profession, the study then turns to the next logical question: How can this gap be addressed? The proposed answer is clear—through education. Embedding cybersecurity topics and a cybersecurity-conscious mindset into architectural curricula is an essential step toward equipping future architects with the knowledge, values, and practical skills needed to design secure and technologically integrated environments.

This study aims to investigate this very issue by examining whether and how leading universities worldwide have incorporated cybersecurity themes into their architecture programs. The hypothesis is that cybersecurity is either insufficiently represented or entirely absent in current architectural education frameworks, and this study seeks to test that hypothesis through a thematic analysis of selected course curricula.

Based on all the above, the purpose of this study is to point out the place of cybersecurity within architectural education. Since it is not feasible to examine all universities in the world that have architecture programs, the scope of the study has been limited to the undergraduate, master’s, and doctoral curricula of the top five universities worldwide in the field of architecture, as ranked by QS as of 2024. The research population has been defined as the compulsory and elective courses offered in these programs, along with their content. Both undergraduate and graduate-level courses were evaluated together. The method used in this study is thematic content analysis. Thematic content analysis is a method that focuses on the systematic examination of qualitative data to identify, analyze, and report recurring patterns of meaning (themes) within the data. This approach allows the researcher to engage with the data and generate meaning within a particular context (Braun & Clarke, 2006). Thematic analysis is especially useful in studies based on participant narratives, written documents, or records, as it enables the data to be organized into meaningful structures. In this study, the thematic framework used was "cybersecurity". The keywords “cybersecurity”, “cyber security”, “digital security”, and “security” were searched in the course titles, course descriptions and contents[3].

2. The Significance of Cybersecurity Culture in Architecture

Architecture, as a profession that designs, shapes, and builds the physical environment required for people to live, work, have fun and meet their needs, is a discipline that is increasingly intertwined with technology and digitalization. With the inclusion of information and communication technologies in building design, the concept of “smart building” has emerged and is gaining increasing popularity.

The influence of popular culture on the increasing preference of smart buildings is undeniable. The living spaces shown in movies, TV series and especially on social media are depicted and encouraged as high-tech, energy-efficient buildings that facilitate human life. Smart buildings have become a symbol that complements the modern lifestyle with the possibilities and conveniences they offer, from energy management to automatic lighting, remote control devices and security systems. As popular culture portrays this vision as an appealing standard of living, the preference for smart buildings in architectural design has accelerated.

Furthermore, smart buildings have become a preferred choice as they provide solutions to address the pressing issues of high energy consumption and carbon emissions, which are among the most significant challenges faced by the world today in the context of the climate crisis and global warming. By monitoring and optimizing energy consumption in real time with smart sensors and automation systems, these buildings prevent waste of resources and offer a more sustainable living model.

The concept of sustainability, which is intensely focused on in the field of architecture, has led to the design of more than ever “sustainable” architectural buildings in recent years. Thanks to the integration of technology, functional, sustainable and user-friendly buildings can now be constructed. A prominent example of this is The Crystal building in London, designed by Wilkinson Eyre Architect and completed in 2012. This building provides solar energy, heat pumps, recycles rainwater and blackwater, and has a design that aims to make maximum use of natural light. Apart from all these features, it is a “smart building” that has sensors, automation systems and software that manages these features in the most efficient way and is connected to a local and external network.

The growing use of cutting-edge technologies in architectural design and implementation, as in the case of The Crystal building heightens and intensifies the criticality of cybersecurity awareness within the field of architecture. The computer systems, internet connections, sensors, and other hardware and software used to manage smart buildings introduce numerous potential and unpredictable cybersecurity vulnerabilities that must be addressed. If a crash or security breach occurs in these systems, the functionality, efficiency and user comfort provided by the architectural design can be

[3] This approach was chosen to ensure methodological consistency, to rely on commonly used terms in the literature and industry, and to frame the research within a widely accepted conceptual framework. While related topics such as data privacy, network security, and risk management are connected to cybersecurity, they were considered outside the scope of this study.

compromised in an optimistic scenario, leading to disruptions in building operations, cost increases and security risks.

While there are still a limited number of projects that directly integrate cybersecurity in architectural design, some pioneering structures that focus on the security of digital infrastructures offer remarkable examples in this field. Particularly, public buildings, data centers and critical infrastructure facilities stand out with design strategies that address both physical and digital security against cyber threats. For example, Facebook's Luleå Data Center in Sweden stands out with its spatial organization that supports not only energy efficiency but also cyber security protocols. The building combines physical security layers (perimeter barriers, controlled access areas) with digital security infrastructure, ensuring that the hardware inside the building is accessible only by authorized personnel. The fact that the design is organized in accordance with the principles of transparency and access control is directly related to the security of digital networks in the physical environment (Harding, 2015). Similarly, in high-security public projects such as the NSA's Utah Data Center, architectural design is integrated with principles such as electromagnetic isolation, cyber-resilient data rooms, and separation of security zones through architectural scaling. In these buildings, security has impacted not only the IT infrastructure but also the formal and functional organization of the building. While such projects demonstrate how cybersecurity can be integrated into architectural design, they also point to the importance of architects addressing digital threats as an integral component of the design process. In the face of emerging digital technologies, cybersecurity-sensitive architecture should be considered not only as a technical but also as an ethical and strategic design discipline.

What needs to be questioned at this point is the extent to which architects and architecture students, both actively working in the field and academics, take the vulnerability of the buildings and spaces they design against cyber threats into account. It is possible to assume that architects who only receive architectural education with a traditional approach will lack the technical knowledge necessary to ensure the cybersecurity of buildings and probably experience issues due to the absence of this perspective in the projects they develop. The question of how prepared the architectural designs are planned against ever-evolving cyber threats constitutes the main problem of this study. Particularly considering the findings showing that the risk of cyber-physical attacks on architectural buildings is increasing (Mantha et al., 2020), it is of great importance to examine the level of adoption of cybersecurity approach in the field of architecture.

3. Potential Cyber Security Threats to Architectural Buildings

It is argued that there is a direct correlation between the rate of adoption of smart technologies in architectural design and the increase in cyber security risks. Architects and building designers must take a proactive approach to cybersecurity, integrating it into the overall design process to mitigate these risks and ensure the safety and resilience of the buildings they design. Some of the most common cybersecurity threats faced by architectural systems are as follows:

Malware Injection: The process of placing malicious code into the system by exploiting the vulnerabilities of a system or software. In terms of built areas, it can be defined as an attempt to inject malware into digital control systems of architectural buildings. With the unauthorized access obtained in this way, it is possible to disrupt critical functions of control systems or steal sensitive data. Similarly, malware injected into a system that controls a building's fire alarm, elevator, security cameras or electrical systems can disable fire alarms, lock elevators or overload energy-intensive components such as air conditioning systems, leading to energy waste and even permanent damage to buildings. In 2013, a cyber-attack was carried out against the Target stores in the USA. During the attack, cyber criminals first gained unauthorized access to the heating, ventilation and air conditioning (HVAC) systems of the stores. In the second stage, the company's main network and payment systems were accessed through the HVAC system and the credit card information of millions of customers was stolen. Target had to pay approximately 18 million dollars in compensation after the attack and suffered a major loss of prestige (Majority Staff Report, 2014).

Distributed Denial of Service (DDoS) Attacks: A type of attack that is carried out by sending an excessive amount of traffic from multiple sources simultaneously to disrupt the normal functioning of a target system. Threat actors can launch DDoS attacks to overwhelm a building's digital infrastructure, causing service disruptions and affecting the availability of critical systems. In a 2016 incident in Finland (The Hacker News, 2016), a DDoS attack was launched against the heating systems of two separate residential complexes. In the attack, the buildings' automated building management systems (BMS) were disabled, causing the buildings' heating systems to shut down. As a result of that, the heating systems were switched off and on repeatedly during the attack and the internal temperature of the buildings dropped to dangerously low levels. In this example, along with ensuring software-based network security, the physical isolation of the critical systems might be critical and such measures must be taken into consideration during the architectural design phase. Also, building management systems should have backup control systems that can be manually activated when the internet connection is lost or attacked.

Phishing and Social Engineering Attacks: Phishing is a type of cyber-attack that aims to obtain individuals' sensitive information (e.g. usernames, passwords, credit card information) by pretending to be coming from a legitimate organization, usually via email, text message or fake websites. In social engineering, instead of trying to circumvent security measures with technical methods, the approach is to abuse the trust of victims. Employees of architecture firms can be targeted through phishing attempts or social engineering tactics, and the login credentials obtained in this way can be used to gain unauthorized access to or decipher sensitive information belonging to the firm. London-based Zaha Hadid Architects (ZHA) suffered such a cyber-attack in 2020. Employees of Zaha Hadid Architects were sent emails that appeared to be from official sources and redirected to fake login pages, eventually compromising their login credentials. As a result, the firm faced the theft of some confidential information from its projects, damage to client trust and the loss of intellectual property (Architectural Digest, 2020).

Supply Chain Vulnerabilities: This refers to a cyber-attack on a target by first exploiting the vulnerabilities of its suppliers, business partners or third-party service providers. Such vulnerability can cause security breaches in any link of the supply chain and then spread to the main company and cause widespread damage. In architectural domain, weaknesses such as insecure firmware or inadequate security measures stemming from the supply chain of third-party components used to build and maintain smart buildings can expose the main architectural systems to potential exploitation of threat actors. A 2019 study found that 26.5% of computers controlling smart building automation systems were subjected to cyberattacks in the first half of 2019 (Kaspersky, 2019). The security of a smart building system is directly related to the security of each component in the supply chain and a smart building is as secure as its weakest component in its supply chain. To prevent such attacks, strong security measures need to be taken in the design, procurement and operation of smart building systems.

Physical Attacks: Physical attacks are a tactic used by cybercriminals to bypass digital security systems and damage the infrastructures of organizations by first exploiting the vulnerability in the physical space and then attacking the digital system. In terms of built spaces, the starting point of such attacks is the lack of physical security measures in a building or facility. A concrete example of such an attack is the cyber-attack on Las Vegas Sands in 2014 (The Hacker News, 2014). In this incident, the team that carried out the cyber-attack first gained physical access to an area in the company that they should not have been able to access and then managed to temporarily disable the company's security systems. In the second phase, the attackers caused serious damage to the company's databases and critical digital infrastructure. This type of incident is a lesson for architects and security professionals, especially those working on large-scale construction projects and/or facilities with technology-intensive infrastructure. Automation systems, including communication protocols, intrusion detection systems, and data protection must be securely integrated into the overall architectural security strategy (Stâmâtescu et al., 2020). Architects should take measures at the design stage to ensure that the buildings or facilities being constructed are resilient to attacks of a physical nature that are mainly targeting the digital infrastructure.

Cybersecurity threats are constantly evolving and diversifying. As technology continues to advance, new and more sophisticated cyber-attacks are emerging, posing significant risks to various industries, including the field of architecture. “Security-by-design” approach is vital in addressing the risks identified in complex systems (Hofer et al., 2022), and there is a need to integrate strategies and principles at the design stage that can ensure the safe and resilient design of smart buildings against potential vulnerabilities. Otherwise, serious consequences such as the disruption of management systems, economic losses, operational disruptions, cascading failures and even physical harm might occur (Skarga-Bandurova et al., 2021).

4. Assessing The Academic Readiness for Cybersecure Architecture

Architectural education does not only consist of the transfer of technical knowledge and skills but also has a unique pedagogical approach that aims to develop multifaceted competencies such as critical thinking, design processes, interdisciplinary interaction and spatial awareness. In this context, Schön's (1983) concept of "reflective practitioner" encourages students to act not only in a result-oriented but also process-oriented and critically conscious manner during the design process. This understanding emphasizes experiential learning and creativity in problem solving, especially in design studios. In addition, architectural pedagogy offers an applied and critical learning model that draws from different disciplines with the central role of studio-based education (Salama, 2016). Unleashing students' creative potential, integrating technological developments into architecture, and relating architecture to its social, cultural and environmental contexts are among the primary goals of current educational approaches (Till, 2009). Today, the widespread use of digital design tools and the increase in data-driven architectural practices have made it a necessity to integrate cybersecurity culture into these studio environments. Students' awareness of issues such as digital privacy, data security, intellectual property rights and digital ethics is both a part of their professional responsibilities and a factor that increases the sustainability and reliability of their designs (Floridi, 2013). In this context, integrating cybersecurity culture into design studios will contribute to the training of architects with ethical and technical equipment suitable for the requirements of the digital age.

The continuous increase and diversification of cyber threats reveals the necessity for architects to undergo both theoretical and practical training about cybersecurity. Although it is crucial for both practicing architects and architecture students, who will become the architects of tomorrow, to receive this training, the adoption of cyber security culture by architects while they are still in the education stage is more desirable and will ensure that the smart buildings of the future will be designed more resilient to cyber threats and vulnerabilities. In this study, the intersection point of architecture and cybersecurity is examined and the adoption level of cybersecurity culture in architectural education is evaluated using thematic content analysis.

The curricula, course titles and course descriptions of architecture departments at the top five universities worldwide—ranked under the category “Architecture and Built Environment” in the QS

World University Rankings 2024 (QS World University Ranking, 2024[4])—were included in this review. To ensure geographical diversity, a location-based filtering and grouping strategy was applied to represent different regions of the world. Table 1 below presents the regions, selected universities, their respective rankings, the availability of curriculum and course content, and the findings from the keyword-based review. The keywords used in the analysis were “cybersecurity”, “cyber security”, “digital security” and “security.”

Table 1. Course Content Research on the Concept of “Cybersecurity” in Architecture Education

Region	University	QS Ranking & Overall Score	Curriculum / Course Content Access	Courses covering “Cybersecurity” topics
The Americas	Massachusetts Institute of Technology (MIT)	2 & 95,4	Accessible (MIT, 2024)	Although there are some technology-based course titles such as Environmental Technologies in Buildings, keywords research did not yield any results.
	Harvard University	6 & 87,4	Accessible (Harvard, 2024)	Although keywords research yielded 23 results, when their contents were analyzed, no course directly related to cybersecurity was found.
	University of California, Berkeley (UCB)	9 & 86,7	Accessible (UCB, 2024)	No results were found from keyword research conducted on course titles or contents.
	Columbia University	16 & 79,3	Accessible (Columbia, 2024)	No results were found from keyword research conducted on course titles or contents.
	University of California, Los Angeles (UCLA)	17 & 79,2	Accessible (UCLA, 2024)	In the course titled Environmental Control Systems (411 Environmental Control Systems), comfort control of buildings, heating, cooling, air conditioning systems, plumbing, electricity, lighting, building acoustics, fire and life safety, vertical transportation and system integration are covered, but there is no emphasis on “cybersecurity” concepts.
Europe	University College London (UCL)	1 & 97,4	Accessible (UCL, 2024)	No results were found from keyword research conducted on course titles or contents.
	Delft University of Technology	3 & 93,2	Accessible (Delft, 2024)	No results were found from keyword research conducted on course titles or contents.
	Swiss Federal Institute of Technology Zurich (ETH Zurich)	4 &91,9	Accessible (ETH Zurich, 2024)	No results were found from keyword research conducted on course titles or contents.
	Manchester School of Architecture	5 & 89,2	Accessible (MSA, 2024)	Especially in the second year, there are project courses that aim to develop students' knowledge of design and architecture as well as a context for technology, but there is no direct attribution to cybersecurity topics.
	Politecnico di Milano	7 & 87,3	Accessible (Polimi, 2024)	Although there are courses such as “Smart Cities and Urban Innovation” and “Technology” among the course titles, there is no reference to cybersecurity.
Asia	National University of Singapore (NUS)	5 & 87,6	Accessible (NUS, 2024)	The course (Modern Theories-Contemporary Theories) in the graduate department of the university aims to introduce architecture students to a range of intellectual ideas and theoretical positions and covers nine topics, one of which is “security” and the other is “networks”. Among the universities examined so far, NUS offers the content closest to the research topic.
	Tsinghua University	8 & 86,8	Not Accessible	Not Evaluated
	The University of Hong Kong	12 & 82,2	Accessible (HKU, 2024)	In the course “Building Information Modelling in Architectural Practice”, it is seen that new technological applications and the topic of "security" are discussed.
	Tongji University	13 & 82,1	Accessible (Tongji, 2024)	No results were found from keyword research conducted on course titles or contents.
	The Hong Kong Polytechnic University	14 & 81,3	Not Accessible	Not Evaluated
	The University of Tokyo	15 & 80,8	Not Accessible	Not Evaluated
	Nanyang Technological University	18 & 79,5	Not Accessible	Not Evaluated

[4] The QS World University Rankings is a prestigious and generally recognized ranking system that has been published every year since 2004 by Quacquarelli Symonds (QS), a UK-based organization that assesses the academic performance, research quality and international reputation of universities around the world. The QS World University Rankings are frequently used as an important reference source for evaluating and benchmarking universities and for international collaborations and research funding. The “Architecture and Built Environment” section of the QS Rankings evaluates higher education institutions specializing in fields of architecture, urban design, structural engineering and environmental design.

	Tianjin University	34 & 75,2	Accessible (Tianjin, 2024)	No results were found from keyword research conducted on course titles or contents.
	Seoul National University	36 & 75	Accessible (SNU, 2024)	In the course “Building Information Modeling in Architectural Practice”, it is seen that new technological applications and the topic of "security" are discussed.
Oceania	Royal Melbourne Institute of Technology (RMIT University)	18 & 78,2	Accessible (RMIT, 2024)	A course with the name “Architecture Technology” is offered throughout the first four semesters of undergraduate architectural education. It is stated that the course includes a comprehensive description of modern architectural technologies, and the main objective of the course is to address the connection between architectural design and architectural technology. In addition to this approach, there is no information on the inclusion of cybersecurity topics in the course content.
	The University of Melbourne	24 & 76,9	Accessible (Melbourne, 2024)	Although digital technologies are mentioned in the “Twenty-first Century Architecture” course and building technologies used in complex and large buildings (high-rise buildings, commercial complexes, etc.) are mentioned in the “Applied Architectural Technology” course, it is understood that cybersecurity topics are not included in the course contents.
	The University of Sydney	27 & 76	Accessible (Sydney, 2024)	Although concepts such as thermal comfort in buildings, heat transfer, climate zones, performance of building materials, low energy technologies, water management are covered in the “Architectural Technologies I” and “Architectural Technologies II” courses in the undergraduate department of Architecture and Environment, cybersecurity topics are not included.
	The University of New South Wales (UNSW Sydney)	35 & 75.1	Accessible (UNSW, 2024)	The curriculum includes a group of courses under the title of “digital technology”. Among others, one core course that outstands is “BENV2001 Emerging Digital Technologies” and an elective course that outstand is “ARCH2170 Building Information Management”. Nevertheless, no results were found from keyword research conducted on course titles or contents.
	Curtin University	51-100 The overall score has not been calculated.	Accessible (Curtin, 2024)	No results were found from keyword research conducted on course titles or contents.
Africa*	University of Cape Town	101-150 The overall score has not been calculated.	Not Accessible	Not Evaluated
	Cairo University	51-200 The overall score has not been calculated.	Not Accessible	Not Evaluated
	Alexandria University	201-240 The overall score has not been calculated.	Not Accessible	Not Evaluated
Türkiye **	Istanbul Technical University	101-150 The overall score has not been calculated.	Accessible (Istanbul Technical University, 2024)	No results were found from keyword research conducted on course titles or contents. Although there is a course called “Information Technologies in Architecture”, its content mainly focuses on software and operating systems used in the architectural design process.
Türkiye	Middle East Technical University (METU)	151-200	Accessible (METU, 2024)	No results were found from keyword research conducted on course titles or contents.
Türkiye	Yildiz Technical University	Not included in the QS rankings.	Accessible (YTU, 2024)	No results were found from keyword research conducted on course titles or contents.
Türkiye	Mimar Sinan University	Not included in the QS rankings.	Accessible (MSU, 2024)	No results were found from keyword research conducted on course titles or contents.
Türkiye	Gazi University	Not included in the QS rankings.	Accessible (Gazi, 2024)	No results were found from keyword research conducted on course titles or contents.

* There are only three universities from the African continent in the architecture category of the 2024 QS university rankings.

** Even though there are only two universities from Türkiye in the architecture category of the 2024 QS university rankings, three other leading universities among public universities according to the 2024 ÖSYM placement base points were included in the evaluation to contribute to local academic development.

EVALUATION AND CONCLUSION

The rapidly evolving nature of cybersecurity makes it a field where professionals can easily fall behind if they don't continuously update their knowledge and skills. This dynamic nature presents a significant challenge for curriculum designers, who must create programs that not only provide a strong foundation but also equip students with the ability to adapt to future advancements and emerging threats (Mouheb et al., 2019). Additionally, the need for a continuously updated architectural education that goes beyond skill improvements and establishes a theoretical base for future architects is undeniable (Başarır, 2022). Based on the research findings, it is understood that cybersecurity concepts are insufficiently covered in the architectural education carried out in universities that stand out according to an objective set of criteria from different regions of the world. It is also understood that the architecture students are not guided to acquire a cybersecurity culture throughout their training and thus are not equipped enough to gain this perspective. The lack of exposure to cybersecurity topics during their education years leaves future architects incapable of addressing the growing security challenges that arise with the increasing integration of smart and interconnected technologies into the built environment. In the light of this outcome, cyber threats, which require a proactive and a “secure by design” approach, can often only be addressed after incidents occur. The research findings also indicate that a limited number of architecture schools have begun to incorporate certain topics into their curricula that could help fill the gap. However, these efforts remain relatively limited in scope and have yet to become the norm in architectural education.

It must be given consideration to the fact that due to the lack of integration of cybersecurity culture into architectural education, both the integrity of smart buildings and the built environment remain weakened and the security of people that occupy and use these spaces are jeopardized. Therefore, it is evident that architectural education programs should be re-evaluated through the lens of cybersecurity considerations.

Integrating cybersecurity principles into the architecture curriculum will accelerate and ensure the emergence of a generation of architects who understand the importance of designing resilient buildings that can withstand evolving cyber threats, as suggested by cybersecurity threat models developed specifically for the AEC industry (Mantha et al., 2020).

RECOMMENDATIONS

First and foremost, the lack of interdisciplinary collaboration and knowledge sharing between architects and cybersecurity experts leads to a fragmented approach to security. Therefore, there is a need to encourage interdisciplinary cooperation between architects and cybersecurity professionals.

Within the scope of curriculum development, case studies of architectural firms and projects that have successfully integrated cybersecurity principles into their design processes and outcomes can be included in the courses to address the absence of cybersecurity in the field of architecture more thoroughly. Moreover, elective courses for undergraduate level or courses for graduate level can be developed under the theme of “Cybersecurity Awareness and Culture in Architecture” to introduce future architects to the fundamental concepts of digital safety, risk management, and secure design thinking. At the addendum section, a course proposal titled "Cybersecurity in Design" is presented.

Design studios may also integrate “Security in Design” as a thematic framework for studio projects, encouraging students to tackle real-world challenges that require both architectural and cybersecurity-conscious solutions. In addition, short-term certificate programs, workshops, or even minor programs focusing on cybersecurity could be offered within architecture faculties to raise awareness and build foundational knowledge.

Furthermore, architecture professional associations and chambers could revise their ongoing training programs by integrating “cybersecurity culture” as a module, ensuring that professionals already in the field are also exposed to evolving risks and standards.

On a broader academic level, it would be advisable to conduct more research studies on topics such as cybersecurity practices in smart buildings, integrating cybersecurity approaches and standards into architectural design (Vassigh, 2012), developing comprehensive cybersecurity guidelines and frameworks for the architecture sector, the role of professional associations and regulatory bodies, and evaluating the growing cybersecurity challenges in the built environment.

Additionally, a reverse approach might be the necessary trigger where industry players take the initiative and modify the standards required in the field, which would eventually compel academic institutions to incorporate the new standards into their curriculum. For example, the addition of cybersecurity standards to the existing evaluation categories of LEED (Leadership in Energy and Environmental Design), an international certification system developed by the U.S. Green Building Council (USGBC), would arguably accelerate a similar update in architecture school curricula. Similarly, in BREEAM (Building Research Establishment Environmental Assessment Method), a European-based certification system, it would be advisable to evaluate buildings also in terms of cyber-resilience, alongside components such as energy management, health and well-being, and pollution. The integration of security elements into the R2S (Ready2Services) certification system of the Smart Building Alliance (SBA) which evaluates the readiness of buildings for digital services would also help embed cybersecurity as a key component of future-ready architectural practices and education.

From a local perspective, architectural education in Turkey is largely structured around physical space, aesthetics, structure and urban context. Interdisciplinary and technology-intensive topics such as digital security are usually addressed in a limited way under the titles of “information technologies” or “smart city”. As this study shows, cybersecurity does not find a direct place in the architecture curriculum. Moreover, since cybersecurity is more directly related to fields such as computer engineering, software engineering and information systems, the number of lecturers with such expertise in architecture faculties is quite limited. The majority of architecture students also see cybersecurity as outside their professional fields. This leads to low interest in the subject.

However, in recent years, significant investments have been made in both the public and private sectors in Turkey to promote digitalization. Initiatives such as the “National Cybersecurity Strategy and Action Plan (2024–2028)” and the “National Smart Cities Strategy and Action Plan (2024–2030)” demonstrate that the built environment is also part of this transformation. By aligning architectural education with these strategies, it may be possible to benefit from supporting public funds. Updating education policies, encouraging interdisciplinary collaborations, and increasing academic support will strengthen the cybersecurity dimension in architectural education in Turkey. Furthermore, the digital competencies of younger generations can facilitate the transfer of technical knowledge in topics such as cybersecurity.

Compliance with the Ethical Standard

Conflict of Interests: The author(s) declare that they do not have a conflict of interest with themselves and/or other third parties and institutions, or if so, how this conflict of interest arose and will be resolved, and author contribution declaration forms are added to the article process files with wet signatures.

Ethics Committee Permission: In this article, ethics committee approval is not required, and a consent form affirming that a wet-signed ethics committee decision is not necessary has been added to the article process files on the system.

Financial Support: No financial support was received for the study.

REFERENCES:

Architectural Digest. (2020, September). Zaha Hadid Architect was the Victim of a Ransomware Attack. https://www.architecturaldigest.com/story/zaha-hadid-architects-was-the-victim-of-a-ransomware-attack.

Başarır, L. (2022). Modelling AI in Architectural Education. Gazi University Journal of Science, 35(4), 1260–1278. https://doi.org/10.35378/gujs.967981

Braun, V., Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Boyes, H. A. (2014). Cyber Security of Intelligent Buildings: A Neview. Engineering & Technology Reference. https://doi.org/10.1049/etr.2014.0008

Ciholas, P., Lennie, A., Sadigova, P., & Such, J. M. (2019). The Security of Smart Buildings: A Systematic Literature Review, ArXiv, 1-50. https://doi.org/10.48550/arXiv.1901.05837

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13-21.

Columbia. (2024, September). Architecture Department Course Descriptions. https://architecture.barnard.edu/architecture-department-course-descriptions.

Delft. (2024, November). Bachelor of Architecture, Urbanism and Building Sciences. https://www.tudelft.nl/en/onderwijs/opleidingen/bachelors/bk/bachelor-of-architecture-urbanism-and-building-sciences

ETH Zurich. (2024, September). Teaching Areas & Categories. https://arch.ethz.ch/en/studium/studienangebot/bachelor-architektur/lehrgebiete.html

Floridi, L. (2013). The Ethics of Information. United Kingdom: Oxford University Press.

Gazi. (2024, October). Mimarlık Programı Bilgileri. https://obs.gazi.edu.tr/oibs/bologna/index.aspx?lang=tr&curOp=showPac&curUnit=10&curSunit=106060482#

Harding, L. (2015). The Node Pole: Inside Facebook's Swedish Hub near the Arctic Circle. https://www.theguardian.com/technology/2015/sep/25/facebook-datacentre-lulea-sweden-node-pole

Harvard. (2024, October). Courses. https://www.gsd.harvard.edu/courses/?department=architecture

HKU. (2024, December). Architecture Introduction. https://www.arch.hku.hk/programmes_/arch/.

Hofer, F., Russo, B. (2023). Architecture and Its Vulnerabilities in Smart-Lighting Systems. In: Vershinin, Y.A., Pashchenko, F., Olaverri-Monreal, C. (eds) Technologies for Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3-031-05516-4_10.

Istanbul Technical University. (2024, September). Ders Planları. https://obs.itu.edu.tr/public/DersPlan/

Hollander, J. B., & Sussman, A. (2018). Why Architecture Education Needs to Embrace Evidence-Based Design, Now. Architectural Digest.

Jacob, J., Peters, M.L., & Yang, T.A. (2019). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. Neuromorphic Computing Symposium.

Kaspersky. (2019, September). Smart Buildings Threat Landscape: 37.8% Targeted by Malicious Attacks in H1 2019. https://www.kaspersky.com/about/press-releases/smart-buildings-threat-landscape

Kostešić, I., & Jukić, T. (2024). Institutionalized Interdisciplinary Approaches in Architectural and Design Education. Prostor: A Scholarly Journal of Architecture and Urban Planning, 32(1), 1–186. https://doi.org/10.31522/p.32.1(67).7

Kim, E., Kwon, J., Yoon, J., & Agogino, A.M. (2019). Embedding Cybersecurity Into Design Education: Increasing Designers' Awareness of Cybersecurity Throughout the Design Process. Volume 3: 21st International Conference on Advanced Vehicle Technologies; 16th International Conference on Design Education.

Lawrence-Fowler, W.A. (2013). Multi-disciplinary Approach to Cyber Security Education.

Mylrea, M., Gourisetti, S. N. G., Nicholls, A, (2017). An Introduction to Buildings Cybersecurity Framework, In 2017 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1-7. https://doi.org/10.1109/SSCI.2017.8285228.

Majority Staff Report, (2014, September). A "Kill Chain" Analysis of the 2013 Target Data Breach. September https://www.emacromall.com/reference/A-Kill-Chain-Analysis-of-the-2013-Target-Data-Breach.pdf.

Mantha, B., de Soto, B. G., & Karri, R. (2021). Cyber Security Threat Modeling in the AEC Industry: An Example for the Commissioning of the Built Environment. Sustainable Cities and Society, 66, 102682. https://doi.org/10.1016/j.scs.2020.102682

Melbourne. (2024, October). Architecture. https://msd.unimelb.edu.au/about/disciplines/architecture

METU. (2024, August). Courses Given by the Department of Architecture. https://catalog.metu.edu.tr/prog_courses.php?prog=120.

MIT. (2024, November). Classes. https://architecture.mit.edu/classes

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity Curriculum Design: A Survey. Transactions on Edutainment XV, 93-107. https://doi.org/10.1007/978-3-662-59351-6_9

MSA. (2024, October). Studying At Manchester School of Architecture. https://www.msa.ac.uk/study/

MSU. (2024, December). 2024-2025 Öğretim Yılı Öğretim Planı Ders Programı Ders Bilgi Formları. https://msgsu.edu.tr/wp-content/uploads/2024/10/2024_2025_MIMBOL_DERSKATALOGU.pdf

NUS. (2024, October). Department of Architecture. https://cde.nus.edu.sg/arch/

Pak, B., & Verbeke, J. (2012). Design Studio 2.0: Uugmenting Reflective Architectural Design Learning. Journal of Information Technology in Construction, 502-519.

Polimi. (2024, May). Cerca/Visualizza Manifesto. https://www4.ceda.polimi.it/manifesti/manifesti/controller/ManifestoPublic.do.

QS World University Ranking (2024, August). QS World University Rankings by Subject 2024: Architecture & Built Environment. https://www.topuniversities.com/university-subject-rankings/architecture-built-environment.

Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture, In 29th European Safety and Reliability Conference, 4036-4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

RMIT. (2024, October). Bachelor of Architectural Design - Plan BP250. https://www.rmit.edu.au/study-with-us/levels-of-study/undergraduate-study/bachelor-degrees/bachelor-of-architectural-design-bp250/bp250auscy

Salama, A. M. (2016). Spatial Design Education: New Directions for Pedagogy in Architecture and Beyond. London: Routledge.

Schön, D. A. (1983). The Reflective Practitioner: How Professionals Think in Action. New York: Basic Books.

Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. R. (2021). Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. Frontiers in Computer Science, 3, 1-13. https://doi.org/10.3389/fcomp.2021.614337

Stâmâtescu, G., Stamatescu, I., Arghira, N., & Făgărășan, I. (2020). Cybersecurity Perspectives for Smart Building Automation Systems, In 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 1-5. https://doi.org/10.1109/ecai50035.2020.9223152

SNU. (2024, November). Undergraduate Program. https://architecture.snu.ac.kr/academics/undergraduate-program/.

Statistica. (2024, December). Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023, with Forecasts from 2024 to 2033. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Sydney. (2024, November). School of Architecture, Design and Planning. https://www.sydney.edu.au/handbooks/architecture.html.

Taneja, P., & Kumar, B. (2024). Architecture Education Towards a Sustainable Future: A Review. ShodhKosh: Journal of Visual and Performing Arts, 2582-7472. https://doi.org/10.29121/shodhkosh.v5.iICoMABE.2024.2158

The Hacker News. (2014, October). Las Vegas Sands' Casino Network hit by Destructive Malware. https://thehackernews.com/2014/12/las-vegas-casino-hacked.html.

The Hacker News. (2016). DDoS Attack Takes Down Central Heating System Amidst Winter in Finland. Retrieved October 12, 2024, https://thehackernews.com/2016/11/heating-system-hacked.html.

Tianjin. (2024, August). Undergraduate Program. https://t-arch.tju.edu.cn/PROGRAMMES/Architecture/Undergraduate.htm

Till, J. (2009). Architecture Depends. Cambridge: MIT Press.

Tongji. (2024, October). English Program. https://caup.tongji.edu.cn/caupen/_t1428/33804/list.psp

UCB. (2024, October). Courses. https://ced.berkeley.edu/arch/courses.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a Cyber Security Culture: Current Practices and Future Needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

UCL. (2024, October). Study. https://www.ucl.ac.uk/bartlett/architecture/study.

UCLA. (2024, August). Academics Fall 2024 Courses. https://aud.ucla.edu/academics/fall-2024-courses.

Vassigh, S., Zhu, Y., & Newman, W. (2012). Leveraging Cyber-infrastructure to Transform Building Science Education. Journal of Architectural Engineering Technology, 1(2), 1-9. https://doi.org/10.4172/2168-9717.1000105.

YTU. (2024, November). Mimarlık Lisans Programı (%30 İngilizce). http://bologna.yildiz.edu.tr/index.php?r=program/view&id=50&aid=38.

ADDENDUM:

A Sample Course Proposal

Course Title: Cybersecurity in Design

Course Description: This is a 4th-year undergraduate or graduate level course in architecture education. This course highlights the emerging threats and areas of responsibility encountered in the digital age of architectural education. In an environment where technologies such as smart buildings, digital architecture, IoT (Internet of Things), and BIM (Building Information Modeling) are becoming widespread, architects are responsible not only for physical security but also for digital security. The aim of this course is to help students recognize cybersecurity risks within the context of the digitized built environment and architectural design processes, and to integrate these risks into their design thinking.

Suggested Course Content and its Integration into the Curriculum:

Table 2. Suggested Course Content for Cybersecurity Design Course

WEEK	TOPIC
1	What is cybersecurity, what is cybersecurity culture, and how does it relate to architecture?
2	Digital architecture, smart buildings, and IoT-based structures
3	The relationship between physical design and digital security
4	Types of cyber threats and case examples
5	Cybersecurity in smart cities: risks at the urban scale
6	Building automation systems and cybersecurity: risks at the building scale
7	Data security in BIM (Building Information Modeling) processes
8	Secure Design Protocols: ISO/IEC Standards and Guidelines
9	Ethics, privacy, and digital human rights discussions
10	Applied case studies
11	Design concept development
12	Scenario development on security vulnerabilities and architectural interventions
13	Project presentations and critiques
14	Final presentations

Project Suggestions for Final Presentations:

- Designing a data center that integrates both physical and digital security
- IoT security integration in a smart residential or office building
- Planning data flow security in a BIM-based project
- Designing a public space with a secure digital infrastructure
- Crisis response structures with architectural scenarios resilient to cyberattacks