جامعة نيويورك أبوظبي

NYU | ABU DHABI

Intro

Cybersecurity Implications of Construction 4.0

Dear participant,

The purpose of this short survey (5-8 minutes) is to get a better understanding of the cybersecurity implications due to the automation and digital transformation taking place in the Architecture, Engineering, Construction, and Operations (AECO) industry.

This survey is better visualized on a PC rather than a mobile device. The information you provide will be kept completely confidential in accordance with the General Data Protection Regulations (GDPR) and used for research purposes only. Any identifying personal and organizational data will not be revealed in the research outputs or shared with third parties.

Upon your request, we will send you a summary of the findings from this survey.

Thank you for participating!

Sincerely,

Borja Garcia de Soto, PhD, PE

New York University Abu Dhabi, UAE

Abel Maciel, AR, EngD, RIBA, ARB

The Bartlett Faculty of the Built Environment, University College of London, UK

Alexandru Georgescu, PhD

National Institute for Research and Development in Informatics, ICI Bucharest, Romania

Bharadwaj Mantha, PhD

New York University Abu Dhabi, UAE

Žiga Turk, PhD

University of Ljubljana, Slovenia

About the participant

To better understand the legislation relevant to your organization, please select the country in which the main office of your organization is located.

To better understand how your organization considers security systems, please indicate in which country(ies) your organization operates, or provides services and/or products. *(Please select all that apply)*

** Same as above
Afghanistan
Albania
Algeria
Andorra
Angola
Antigua and Barbuda
Argentina
Armenia
Australia

What is the main industry (vertical) of your organization?

- Construction (AECO)
- Information and Communication Technology (ICT)
- Manufacturing
- Transport
- Education
- Real Estate
- Legal
- Government
- Financial Services
- Other (please specify)

What is the main activity overlap of your organization in relation to the AECO industry? *(Please select all that apply)*

- [ ] Architecture
- [ ] Engineering
- [ ] Construction management
- [ ] Contracting
- [ ] Facilities management
- [ ] Client organization (e.g., Developer)
- [ ] Research & Development
- [ ] Software development
- [ ] _____ Other (please specify)

Which construction sector is your organization mostly involved with? *(Please select all that apply)*

- [ ] **General Building**
  (Includes commercial buildings, offices, stores, educational facilities, government buildings, hospitals, medical facilities, hotels, apartments, housing, etc.)
- [ ] **Transportation**
  (includes airports, bridges, roads, canals, locks, dredging, marine facilities, piers, railroads, tunnels, etc.)
- [ ] **Industrial Process**
  (includes pharmaceutical plants, chemical plants, food and other processing plants, pulp and paper mills, steel mills, non-ferrous metal refineries, etc.)
- [ ] **Manufacturing**
  (includes auto assembly, electronic assembly, textile plants, etc.)
- [ ] **Power**
  (includes thermal and hydroelectric power plants, waste-to-energy plants, transmission lines, substations, cogeneration plants, etc.)
- [ ] **Petroleum**
  (includes refineries, petrochemical plants, offshore facilities, pipelines, etc.)
- [ ] **Telecommunications**
  (includes transmission lines and cabling, towers and antennae, data centers and web hotels, etc.)
- [ ] **Water Supply**
  (includes dams, reservoirs, transmission pipelines, distribution mains, irrigation canals, desalination and potability treatment plants, pumping stations, etc.)
- [ ] **Sewerage-Solid Waste**
  (includes sanitary and storm sewers, treatment plants, pumping plants, incinerators, industrial waste facilities, etc.)
- [ ] **Hazardous Waste**
  (includes chemical and nuclear waste treatment, asbestos and lead abatement, etc.)

What is the size of your organization? *(Please select the number of full-time employees)*

- ○ Less than 10 (micro)
- ○ 10-49 (small)
- ○ 50-249 (medium)
- ○ Over 250 (large)

On average, on how many projects is your organization involved per year?

- ○ 1-10
- ○ 11-20
- ○ 21-40
- ○ 41-60
- ○ Over 60

Gauge awareness

Are you concerned about cybersecurity in the AECO industry?

- ○ Yes, significantly
- ○ Yes, somewhat
- ○ Maybe a little
- ○ No
- ○ I don't know / never thought about it

Are your colleagues and/or co-workers concerned about cybersecurity in the AECO industry?

- ○ Yes, significantly
- ○ Yes, somewhat
- ○ Maybe a little
- ○ No
- ○ I don't know

On a scale of 0 to 5, 0 being the lowest and 5 the highest, how concerned are you about the following types of cyber-attacks in relation to their potential impact to the AECO industry?

	0	1	2	3	4	5

	0	1	2	3	4	5
Computer viruses / Malware (e.g., malicious software, including spyware, ransomware, viruses, and worms)	○	○	○	○	○	○
Phishing (emails with malicious links, infected attachments, or tricking users into providing sensitive or confidential information)	○	○	○	○	○	○
Man-in-the-middle attack (MitM) (e.g., in unsecure Wi-Fi, attackers can insert themselves between a visitor's device and the network)	○	○	○	○	○	○
Denial-of-service attack (used to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests)	○	○	○	○	○	○
Attack vectors (used to gain access to a computer or network in order to infect it with malware or harvest data)	○	○	○	○	○	○

On a scale of 0 to 5, 0 being the lowest and 5 the highest, what do you think are the most relevant sources of cyber-attacks to the AECO industry?

	0	1	2	3	4	5
Single internal individuals (e.g., 'IP breaches', 'enemy within')	○	○	○	○	○	○
Single external individuals (e.g., 'lone wolves')	○	○	○	○	○	○
Internal groups or coalitions (e.g., 'contractual breaches', 'enemies within')	○	○	○	○	○	○

	0	1	2	3	4	5
External groups (e.g., 'competitors', 'organized crime')	○	○	○	○	○	○
State actors and proxies (e.g., governments)	○	○	○	○	○	○

Has your direct work, or your organization as a whole, been affected by a cybersecurity-related incident?

Examples of cybersecurity incidents can be described as 'data breach', 'unauthorized access', 'malware attack' among other illicit activities.

	Yes	No	I don't know / I am not sure
My direct work was affected	○	○	○
My organization as a whole was affected	○	○	○

Please describe the nature of the cybersecurity-related incident(s), to whatever extent possible, especially highlighting its/their type and implications.

Does your organization have any emergency plan to deal with cybersecurity breaches?

- ○ Yes
- ○ No
- ○ I don't know / I am not sure

Please describe the emergency plan to deal with cybersecurity breaches, to whatever extent possible:

Are you familiar with any of the following cybersecurity protocols and their application to the built environment? (NIST, NIS, IET, PAS)

	Very familiar	Somewhat familiar	Not familiar, but aware of it	Never heard of it
NIST - National Institute of Standards and Technology - Cybersecurity Framework	○	○	○	○
NIS - Network and Information Systems Directive	○	○	○	○
IET - Code of Practice for Cyber Security in the Built Environment	○	○	○	○
PAS 1192-5:2015 - Security-Minded BIM	○	○	○	○

Does your organization have a cybersecurity plan? *(Either developed independently or based on national or international protocols such as NIST, NIS, IET, PAS)*

- ○ Yes, developed BASED on national or international protocols
- ○ Yes, but NOT BASED on national or international protocols
- ○ No, but we are contemplating to develop one
- ○ No, and we are not contemplating to develop one
- ○ I don't know

Do you think your organization would benefit by having a cybersecurity plan in place?

- ○ Yes
- ○ No
- ○ I don't know

Which national or international protocol(s) have been used for your organization's cybersecurity protocol? *(Please select all that apply)*

- ☐ NIST - National Institute of Standards and Technology - Cybersecurity Framework
- ☐ NIS - Network and Information Systems Directive
- ☐ IET - Code of Practice for Cyber Security in the Built Environment
- ☐ PAS 1192-5:2015
- ☐ _____ Other
- ☐ I don't know

Is your organization's cybersecurity operational?

- ○ Yes, the plan is fully operational
- ○ Yes, the plan is partially operational
- ○ No, the plan is not operational
- ○ I don't know

What is the reason for your organization’s initial introduction of the cybersecurity plan? *(Please select all that apply)*

- ☐ Foresight (preventive and/ or pro-active measures)
- ☐ Due to prior experience (cyber-attacks, breaches, or other cybersecurity incidents)
- ☐ Statutory compliance (national or international levels)
- ☐ Competitive advantage (better services/client value perception)
- ☐ _____ Other (please specify)

Damages and impacts

On a scale of 0 to 5, 0 being the lowest and 5 the highest, how concerned would you be if:

	0	1	2	3	4	5

	0	1	2	3	4	5
There is a breach of project confidentiality from inside the project team?	○	○	○	○	○	○
There is a breach of project confidentiality from outside the project team?	○	○	○	○	○	○
There are unauthorized changes to the project information from inside the project team?	○	○	○	○	○	○
There are unauthorized changes to the project information from outside of the team?	○	○	○	○	○	○

On a scale of 0 to 5, 0 being the lowest and 5 the highest, how dangerous would it be if:

	0	1	2	3	4	5
There is unauthorized access to controls and equipment during commissioning or building operations (e.g., BMS; HVAC system; computer network, CCTV, IoT sensors)	○	○	○	○	○	○
There is unauthorized access to site controls and equipment of a project during construction (e.g., tower cranes, drones, autonomous/self-driving forklifts/diggers/trucks)	○	○	○	○	○	○
There is unauthorized access to project-related information via the BIM Common Data Environment (CDE) (e.g., files, documents, cost control, contracts, BIM, specifications, etc.) during any phase of the project	○	○	○	○	○	○

	0	1	2	3	4	5
There is unauthorized access to the organization-related information (e.g., employee information, financials, bank accounts, etc.)	○	○	○	○	○	○
There is unauthorized access through your organization's ICT network to third-party information (e.g., clients, suppliers, vendors)	○	○	○	○	○	○

Comments

Comments or suggestions

The integration of new technologies and the digitalization of the AECO industry is quickly evolving. Although there are many benefits to that, there are also new cybersecurity implications and risks.

Please use the space below if you want to provide any insights, comments, opinions, or suggestions related to the cybersecurity implications of Construction 4.0.

Conclusion

What is your level of seniority in your organization?

- ○ Senior, Executive or Top-Level Management
- ○ Middle-Level Management / Director

- ○ Manager / Advisor
- ○ Entry level / Staff
- ○ [ ] Other (please specify)

How many years have you been in your current role?

- ○ Less than 2
- ○ 2-5
- ○ 6-10
- ○ More than 10

May we contact you for further research? We will be conducting in-depth interviews about cybersecurity and emergent technologies in construction. *(If yes, you will be asked to provide your Email)*

- ○ Yes
- ○ No

Would like to receive a summary with the preliminary findings from this survey? *(If yes, you will be asked to provide your Email)*

- ○ Yes
- ○ No

Please provide your contact information below. Your name or e-mail address will be kept confidential and they will not be linked to your questionnaire responses or shared with third parties.

Title

Name

Email

Powered by Qualtrics