Deloitte.

德勤

2022 Construction Predictions

Issue 1

March 2022

MAKING AN IMPACT THAT MATTERS since 1845

Building cybersecurity in the construction industry

Why should construction and infrastructure companies shape a resilience strategy in the age of ransomware warfare

Introduction

Construction 4.0 is transforming the industry landscape in an unpredictable way. Artificial intelligence (AI) and advanced analytics (AA) are enabling new efficiency and creating new risk management paths.

Cyber-physical systems should enhance the delivery and management of connected construction facilities for both greenfield and brownfield projects. Digital security will be considered essential to avoid disruption and raise resilience.

According to most analysts, the construction and infrastructure (C&I) industry will grow in 2022[1]. C&I will support nations' growth plans and will drive investment across healthcare, public safety, and other public infrastructure. Since the pandemic has shifted this sector from traditional legacy constricted IT to digital acceleration plans, cyber security standpoint needs to evolve from perimeter-based to data oriented.

In the age of ransomware warfare, the integrity and availability as essential attributes of both AA and AI should be preserved. Best in class operators must protect their process know-how if they want to preserve their innovation investment advantage over their competitors. In this context, data governance should embrace classification and security as a priority.

Digital Identity.
According to Gartner, "attacks on organizations in critical infrastructure sectors have increased dramatically, from less than 10 in 2013 to almost 400 in 2020 — a 3,900% increase"[2]

C&I is facing many challenges: the pandemic crisis, the Green Revolution, and supply shortages to name but a few. To cope with so many trials and tribulations, C&I should transform its entire value chain. Vertical integration needs to break barriers throughout the chain. Digital identity and privilege access management should be deployed to ensure access control while integrating suppliers and contractors.

Secure backups.
The adoption of Building Information Modeling (BIM) and digital twins will require special attention to ensure integrity and availability of data. Network segmentation and log monitoring should be deployed to minimize the business impact of a cyber-attack. Secure backup environments, both on-site or cloud-based, will enable data to be restored, if necessary, enabling production and time to market to continue uninterrupted.

Cyber-physical systems (CPS) security.
Companies who have invested heavily to expand thier business portfolio, offering concessions, water and waste management, energy systems and plants, maintenance and asset management solutions, are embedding CPS wherever they can.

1. "What the 2021 construction demand means for 2022", published 13 December 2021 https://www.tomorrowsworldtoday.com/2021/12/13/what-the-2021-construction-demand-means-for-2022/ Accessed 20 December 2021.
   Australian Industry and Skills Committee, "Construction, overview" last updated 18 January 2022 https://nationalindustryinsights.aisc.net.au/industries/construction Accessed 18 January 2022.
   James Leggate "Economist Projects 'Very Busy' 2022 for Construction Industry", published 9 December 2021 https://www.enr.com/articles/53205-economist-projects-very-busy-2022-for-construction-industry Accessed 20 December 2021.
2. Analyst(s): Katell Thielemann, Wam Voster, Barika Pace, Ruggero Contu, Richard Hunter, Critical Infrastructure in Focus, published 17 November 2021 https://www.gartner.com/en Accessed 20 December 2021.
3. Dennis Scimeca "Prepare For More Cyberattacks in 2022" published 15 December 2021 https://www.industryweek.com/technology-and-iiot/cybersecurity/article/21184175/prepare-for-more-cyberattacks-in-2022 Accessed 21 December 2021.
   Steve Morgan "Cybersecurity Jobs Report: 3.5 Million Openings In 2025", published 9 November 2021 https://cybersecurityventures.com/jobs/ Accessed 21 December 2021 accessed 28 July 2020.

This development will extend the exposure to cyberthreats. While "traditional" IT security is nowadays hard to maintain, CPS security is even harder to achieve. Cyber attacks targetting CPS in operational technology (OT) environments have evolved from process disruption, such as shutting down a water plant, to compromising the integrity of industrial environments. These threat scenarios may be amplified by faster 5G connectivity. In order to respond to the new CPS threat landscape, companies should develop a cyber-physical systems security strategy with a holistic approach where OT, the Internet of Things (IoT), the industrial Internet of Things (IIoT) and IT security are managed as part of a single coordinated effort.

Cyberattacks are expected to grow over the next five years as well as the cybersecurity talent shortage[3].

Cyber security management as a service.
This will be the way many sectors such as C&I acquire protection capabilities for their operations. Cybersecurity governance requires multidisciplinary resources to be effective. Self sufficiency approaches in cybersecurity are no longer an option, C&I players should invest in hybrid models to ensure they reach a proper level of maturity in cyber security.

Four domains of information security will drive the cyber agenda in 2022:
risk assessment and business impact analysis, vulnerability assessment tooling and red teaming, security awareness and training, and security incident and event management.

The construction and infrastructure Industry should make cybersecurity a part of their good corporate governance strategy to support building trust among stakeholders and investors.

Written by

Gianluca D'Antonio
Partner, Risk Advisory
Deloitte Spain
gdantonio@deloitte.es

Deloitte China Contacts

Ricky Tung
Industrial Products & Construction Sector Leader
Deloitte China
rictung@deloitte.com.cn

Lily Yin
Construction Sector Leader
Deloitte China
lilyin@deloitte.com.cn