Cybersecurity for Architects

3 PDH/ 3 CE Hours/ 3 AIA LU Hours

AIAPDH191
I. Final Exam Answer Sheet

1. The World Economic Forum’s Centre for Cybersecurity was established to:
   a. Defend economic policies
   b. Shape the future of cybersecurity and digital trust.
   c. Field a baseball team
   d. Work on world hunger

   a. Technology can overcome all obstacles
   b. One should have not fear
   c. Cyber threats and events can happen to anyone
   d. Design is ascending in the 2020s.

3. Typical tools used in cybersecurity include
   a. Drafting tables
   b. Anti-virus/anti-malware software
   c. Quill pens
   d. Specification handbooks.

4. The following are examples of OT (Operational Technologies):
   a. Electrical Grids
   b. Basketball courts
   c. Collaborative websites
   d. Professional societies

5. Accounts & Billing, knowledge base, financial records, etc. are examples of virtual assets, otherwise known as:
   a. On site investigation
   b. Free trade items
   c. IT Information Technology
   d. Sustainable activities
6. Cybersecurity is considered to have begun with what software program?
   a. Word Perfect
   b. The Creeper
   c. Multiplan
   d. Microsoft Powerpoint

7. Ray Tomlinson wrote ________, a program to chase the first self-replicating software and delete it
   a. Sketchup
   b. Quicken
   c. Reaper
   d. Turbo Tax

8. One of the most powerful first examples of malware, the Morris worm, was designed for what purpose?
   a. Optimize computer operating systems.
   b. Count cards in Las Vegas
   c. BIM checking
   d. Gauge the size of the internet.

9. Examples of the torrent of malware activity growing rapidly are ALL BUT the following:
   a. By 2014 over 500,000 per day
   b. In 1990s, 10s of thousands
   c. In 2007, 5 million per year
   d. Once every month

10. The WannaCry ransomware attack on May 12, 2017 had the following effect
    a. Was a baby in distress
    b. Minimal impact
    c. Within 24 hours infected more than 230,000 computers in over 150 countries
    d. Was limited to Mexico

11. The American Medical Collection Agency (AMCA) Breach between August 2018 and March 2019 exposed
    a. Flaws in health reform
    b. 7.7 million LabCorp customers data
    c. Nothing significant
    d. Political rifts in the Affordable Care Act
12. Cyber-resilience, according to Gartner, will mean threats are significant given that __________ internet-connected devices are expected by 2020.
   a. A few here and there
   b. 20.4 billion
   c. Slow moving
   d. Less than 50,000.

13. ENR (Engineering News Record)’s assessment of the readiness of the design and construction industry is that the following are true EXCEPT
   a. Don’t think GC’s and CM’s are worried enough about the impact a cyber incident can have
   b. The view is bleak
   c. Most experts are optimistic
   d. Risk managers are too often not technical enough

14. Construction Dive in 2016 reported __________ per cent increase in ransomware attacks.
   a. 1
   b. 5
   c. 20
   d. 400

15. IT, ICT, and OT describe all but the following with respect to cybersecurity
   a. Industrial Control Systems
   b. Information technologies
   c. Positions on a basketball team
   d. Operational technologies

16. Seriously damaging examples of malware, as described by Michael Chipley in the Whole Building Design Guide, are all EXCEPT
   a. Stuxnet
   b. Software bugs
   c. Shamoon
   d. Flame

17. Although 5G networks did not exist at the time, the NotPetya malware attacked caused __________ in corporate losses in 2017
   a. Minimal
   b. $500,000
c. Over $10 billion  
d. None at all.

18. McKinsey in their 2016 report included all but the following in trends that will shape the construction industry  
a. Construction flaws and errors and admissions  
b. Digital collaboration and mobility  
c. Next-generation 5-D information modeling  
d. Future-proof design and construction

19. Trimble recommends “4 Keys to Thwarting Cyber Criminals” that include all but the following  
a. Backup files  
b. Consistent Training and Updates  
c. Write passwords on sticky notes  
d. Deploy multi-factor authentication

20. Which of the following is an AIA Trust and Victor Inc. recommendation for all professionals, based on information provided by IBM’s 2015 Cyber Security Intelligence Index:  
a. Build a risk-aware culture  
b. Manage and report all incidents  
c. Patrol the neighborhood  
d. All of the above
Cybersecurity for Architects
Opportunities and Challenges

By Stephen R Hagan FAIA

4/12/2020

Course Description and Learning Objectives

Course Description

Cybersecurity poses a unique and emerging challenge and new dimension to Architects and Architectural Practice.

In this course, you will:
1. Explore current trends in cybersecurity and their impact on the profession of architecture and urban planning
2. See how responses to cyber threats are making dramatic improvements in the lives of architects' clients.
3. Understand how architectural and consulting firms and organizations, with input from experts, are making game changing strides in risk management and cybersecurity
4. Stay ahead of the sea change in an industry that is already feeling the impact of cybersecurity

Learning Objectives

1. Upon completion, participants will be able to understand the domain of cybersecurity, and how cyber threats pose dangers to their architectural practice, their teams, and their clients as well. While these cyber threats can affect the value of the built environment in terms of safety, occupant comfort, and well-being, cybersecurity enables the architect and architectural practice to protect the value of the built environment in these same terms, often using data and technology feedback for human-centric and experiential design processes.

2. Upon completion, participants will be able to learn what critical steps are needed by path-breaking and leading firms in response to these cyber threats. Many firms have transformed their practices through risk management techniques and processes, mitigating problems, as well as improving quality and integration of design and construction documents. These path-breaking firms are needing an emphasis and focus on cybersecurity is critical to a) ensuring the physical, emotional, and social well-being of occupants, users, and any others affected by their projects b) protecting occupants, users, and any others affected by their projects, and c) enable equitable access, elevate the human experience, encourage social interaction, and benefit the environment.
3. Upon completion, participants will be able to understand how the built environment, form and function of architecture, and everything from small components to entire buildings to regions and urban scale can be affected by cyber threats. The course will explore both the physical and virtual world and the effect of these cyber threats on a) protecting occupants, users, and any others affected by buildings or sites from harm and b) improve the physical, emotional, and social well-being of occupants, users, and any others.

4. Upon completion, participants will be able to take key ideas back to the office on Monday and create their own Cybersecurity Strategic Plans for their in-house projects and firm-wide business planning. Plans will include building systems, construction contract administration and documents, and design (including urban planning). From pre-design topics such as land use analysis, to utilization of smart city concepts and data for preservation such as historic, reuse, or adaptation, practitioners are making dramatic improvements in the process of urban planning, and seeing positive outcomes for cybersecurity as well. All of these actions resulting from creating and implementing a Cybersecurity Strategic Plan by firms and their associates will inevitably a) improve the physical, emotional, and social well-being of occupants, users of their projects, b) protect occupants, users, and any others affected by buildings or sites from harm (in this case both physical and virtual harm to businesses and individuals, and ultimately c) elevate the human experience, encourage social interaction, and benefit the environment.
Table of Contents

I. Final Exam Answer Sheet ........................................................................................................ 2

II. Introduction and Overview .................................................................................................. 10
   A. What is “Cybersecurity”? ....................................................................................... 10
   B. Cybersecurity from the Beginning ......................................................................... 16
   C. Scale and Size of the Cybersecurity Threat in the U.S. and Worldwide ........ 18
   D. Profile of Cybersecurity Today .............................................................................. 21
   E. Information Technologies (IT) and Cybersecurity .............................................. 24
   F. Operational Technologies (OT) and Cybersecurity .............................................. 25
   G. IT versus OT ......................................................................................................... 27
   H. Game-Changing Technology | Innovation in Cybersecurity ............................. 28

III. Construction Industry Perspective ................................................................................ 30

IV. Construction Industry Perspective on Cybersecurity ................................................... 32
   A. Construction Industry Stakeholders ..................................................................... 32
   B. Built Environment | Digital Transformation | Cybersecurity .......................... 33
   C. Venture Capital | Startups: Investing in Cybersecurity ..................................... 38
   D. Companies | Organizations Influencing Cybersecurity ................................... 39

Construction Industry Perspective ...................................................................................... 44

V. Game Changing Innovation Impacting the Future of Cybersecurity ............................ 46
   A. Artificial Intelligence (AI) and Machine Learning (ML) .................................... 46
   B. Augmented Reality (AR) / Virtual Reality (VR) .................................................. 49
   C. Blockchain ............................................................................................................. 50
   D. Building Information Modeling (BIM) .................................................................. 52
E. Internet of Things (IoT) ............................................................... 53
F. Mobile Devices and APPs .......................................................... 54
G. Venture | Startup Innovations in Construct-tech ....................... 54

IV. Cybersecurity Case Studies in the Construction Industry .......... 59
A. Turner Construction ................................................................. 59
B. Whiting-Turner Contracting .................................................... 59
C. Central Concrete Supply Company and others ......................... 60
D. A Steel Mill in Germany ........................................................... 60
E. Target and Fazio Mechanical ................................................... 60
F. Bird Construction ................................................................. 60
G. U.S. Department of Defense ....................................................... 61

V. Making Your Own Cybersecurity Execution Plan ...................... 64
A. BIM Execution Planning as a Role Model ............................... 64
B. YOUR Cybersecurity Execution Plan ....................................... 66

VI. Conclusion and Path Forward .................................................. 67
A. AIA Trust Recommended Security Essentials ......................... 67
B. Flipboard Magazine “Cybersecurity for Architects” ................. 68

VII. Final Thoughts ........................................................................ 70

Table of Figures ............................................................................. 71

VIII. Bibliography ........................................................................... 72
IX. Chapter Review Questions and Evaluative Feedback ................. 79
X. Author Biography: Stephen R Hagan FAIA ............................... 86
I. Introduction and Overview

This course on cybersecurity for architects provides a broad overview of the concept of cybersecurity. It also takes an in-depth look at some of the details of cyber threats and cybersecurity, particularly with respect to the architecture profession, the construction industry, and more broadly all professionals, organizations, and companies involved in the built environment.

We look first at various definitions of cybersecurity, and establish the stakeholders and where cyber threats are being deployed globally. We then identify seminal sources and organizations that explain the current state of cybersecurity.

The historical context of cybersecurity is investigated and the status of the cyber threats as they have evolved globally is explored. The current state of industry innovation, the onset of game changing innovative technologies, and cybersecurity case studies are also described.

We conclude with an explanation of how to plan your own cybersecurity execution plan, as well as perspectives on the path forward and the future.

Technologies and processes and, ultimately, digital transformation are what are driving the innovation in the design and construction industries and the built environment. The goal is NOT to have cyber threats stymie that innovation.

What is “Cybersecurity”?

The American Institute of Architects (AIA) notes that cyber threats and events “can happen to anyone (An Architect’s Guide to Managing Cyber Threats).” The AIA describes them as “An event on a system or network detected by a security device or application: malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.”

The AIA itself quotes what IBM calls its “X-Force Threat Intelligence Index,” and this report notes disturbing trends in cybersecurity:

- 8.5 billion records were compromised in 2019
- Destructive malware activity shows that this potentially catastrophic malware trend continues to be a rising threat.
A 2000% increase in operational technology (OT) targeting incidents in 2019 “could portend the rising interest of threat actors to attach industrial systems as we move into 2020 (IBM X-Force Threat Intelligence Index, 2020).”

Another definition of cybersecurity, provided by Technopedia, suggests that cybersecurity “…encompasses numerous hardware and software technologies, and can be applied on any level, including personal, corporate or governmental devices or networks (Cybersecurity, 2020).” Typical tools used in cybersecurity include:

- Passwords
- Anti-virus/anti-malware software
- Software patches
- Firewalls
- Two-factor authentication
- Encryption

Critical personnel at a firm using cybersecurity may be a chief security office (CSO) or chief information security officer (CISO).

Wikipedia defines cybersecurity as “security as it is applied to information technology (Cybersecurity information technology list, 2020),” and provides a list of relevant terms, including (explanation of terms are excerpted from (Wikipedia)):

- **Cryptography.** Cryptography refers to the study and practice of communicating securely whilst in the midst of third parties who are adversaries. The emphasis in cryptography is the development and deployment of specific protocols between trust parties in order to prevent the public or third party adversaries from intercepting and reading messages. Some of the examples of applications of cryptography include things like electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

- **Steganography.** Steganography involves concealing a message or file or image or video within another message, file, image or video. The word comes from the latin and greek words that mean “writing” and “covered or concealed”. The term first appeared in 1499 in a treatise by Joahannes Trithemius entitled “Steganographia”, which was actually about cryptography and steganography, disguised as a
book of magic. “The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.”

- **Authentication and access.** In general, before being granted access to a secure website or domain, the user is required to be authenticated. It is defined as “act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing’s identity, authentication is the process of verifying that identity.” Authentication comes from the Greek words for “genuine” and “author”.

- **Public Key Infrastructure (PKI).** PKI refers to “a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.” The primary purpose of PKI is to enable secure electronic transfer of image. This can be used for “a range of network activities such as e-commerce, internet banking and confidential email.”

- **Tools.** Cybersecurity tools and both software and hardware devices to assist in detecting, combating, and mitigating cyber threats. They come in several forms, including
  
  o Network Security Monitoring tools.
  o Encryption Tools.
  o Web Vulnerability Scanning tools.
  o Network Defence Wireless Tools.
  o Packet Sniffers.
  o Antivirus Software.
  o Firewall.
  o PKI Services.

- **Threats.** Cyber threats consist of ransomware, denial of service, phishing, and many other forms.
• **Exploits.** Exploits in terms of cybersecurity are defined as “a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).” Exploits are often used in terms of taking control of a computer system or network and inflicting harm by “exploiting” a vulnerability.

• **Criminal activity.** Although cybersecurity and cyber threats can be a nuisance, when they threaten stability or inflict personal, corporate or economic injury, they are also a crime. Crimes can include: “Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime) Information warfare. Phishing scams.”

• **Nation states.** The term nation state or nation state actors means that various nations around the world have given hackers permission to hack on their behalf. For example, they might be part of a semi-hidden ‘cyber army’ or ‘hackers for hire’ for companies that are aligned to the aims of a government or dictatorship. The physical, cyber and financial damage and mayhem created by nation state actors is fully supported by the sovereign nation and in many instances can be considered an act of aggression or even war.

• **Endpoint protection.** Endpoint protection or endpoint security is a way of protecting a business or personal computer network at the outer boundaries or “end points” where the network connects to the public internet. Whether it is mobile devices such as iphones, ipads or tablets or laptops that are connected to the network, these “end point” connections create a vulnerability for the network they are on. “The endpoint security space has evolved over the last several years away from limited antivirus software and into a more advanced, comprehensive defense. This includes next-generation antivirus, threat detection, investigation, and response, device management, data leak protection (DLP) and other considerations to face evolving threats.”

• **Network protection.** Network Access Protection or network protection is a technology that relies on the health of a system (i.e.,
its level of protection based on downloaded security updates and patches.)

- **Processing protection.** The three pillars of cybersecurity are considered to be technologies, processes and measures. Security of processes is equal to the other two pillars.

- **Storage protection.** Storage protection is also often referred to as “memory” protection and involves controlling access to computer memory to prevent and mitigate cyber threats. “The main purpose of memory protection is to prevent a process from accessing memory that has not been allocated to it. This prevents a bug or malware within a process from affecting other processes, or the operating system itself.”

- **Management of security.** Management of security or more appropriately referred to as “security management” “is the identification of an organization’s assets (including people, buildings, machines, systems and information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets.”

- **Standards, frameworks, & requirements.** These three terms are a catch-all for accredited and authoritative published materials such as the NIST Cybersecurity Framework and other industry-wide and adopted standards to protect user themselves, networks, devices, software and processes from cyber threats. “Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s.”

It is important to note as we define cybersecurity that there is a fundamental difference between cybersecurity for OT (operational technologies) versus IT (informational technologies). These can be further defined as physical assets versus virtual assets, as illustrated in **Figure 1** (Infographic: OT vs. IT Cybersecurity, 2020).
For the most part we will be discussing the virtual assets of design and construction and the cybersecurity aspects of protecting them. But as we get into future game changing technologies, how the virtual blends with the physical environment will raise significant issues for industry stakeholders and make it imperative that all fully understand the implications of both OT.
and IT cybersecurity. The two aspects of OT and IT and will be further discussed below.

**Cybersecurity from the Beginning**

How did the concept of cybersecurity begin? Bob Thomas, a software engineer, was working on a research project and

“…realized that it was possible for a computer program to move across a network, leaving a small trail wherever it went. He named the program Creeper, and designed it to travel between Tenex terminals on the early ARPANET, printing the message “I'M THE CREEPER: CATCH ME IF YOU CAN.”

Ray Tomlinson, another software engineer who also invented email, played around with the creeper program and made it self-replicating—creating the first “computer worm.” Tomlinson then “wrote another program—Reaper, the first antivirus software—which would chase Creeper and delete it.”

Bizarrely, the origins of today’s incredibly destructive cyber threats and even cyber warfare were simple academic experimentations. But from academic exploration, things took a quick turn to dangerous criminal activity. One of the first examples of this activity was in 1986:

“The Russians… quickly began to deploy cyberpower as a weapon. In 1986, the German computer hacker Marcus Hess hacked an internet gateway in Berkeley, and used that connection to piggyback on the Arpanet. He hacked 400 military computers, including mainframes at the Pentagon, with the intent of selling their secrets to the KGB. He was only caught when an astronomer named Clifford Stoll detected the intrusion and deployed a honeypot technique.”

Another seemingly harmless academic exercise to assess the overall size of the internet at the time became a harbinger of the viral era:

“Late in 1988, a man named Robert Morris had an idea: he wanted to gauge the size of the internet. To do this, he wrote a program designed to propagate across networks, infiltrate Unix terminals using a known bug, and then copy itself. This last instruction proved to be a mistake. The Morris worm replicated so aggressively that the early internet slowed to a crawl, causing untold damage.”
The Morris worm had long-term implications for cybersecurity. In fact, Morris himself was the first person who was charged under the Computer Fraud and Abuse Act. That act also led to the creation of an entity called the “Computer Emergency Response Team,” now referred to as US-CERT. That organization, non-profit in nature, is a research center for security issues affecting the entire internet.

Many other, far more damaging, viruses cropped up, and an entire industry grew up around anti-virus software. What began in the early 1980s became a torrent of activity in the 1990s, including scanners to detect these viruses and other malware. The malware samples which, in the 1990s were counted in the 10s of thousands, became as many as 5 million by the year 2007. Then by 2014, it was estimated that over 500,000 unique examples of malware were being produced every day.

Despite these amazing numbers, things got worse. There was a leak of software hacking tools utilized by the National Security Agency (NSA) exposed vulnerabilities in operating system protocols that allowed bad actors to navigate laterally throughout a network undetected for a considerable period of time.

New malware like “EternalBlue,” released by a hacker group named Shadow Brokers, easily avoided detection by even sophisticated protection tools, and was used to devastating effect: for example, the May 12, 2017 “WannaCry” ransomware attack.

“It’s hard to recall a bigger shock to the IT community than WannaCry, ‘the biggest ransomware offensive in history.’ Within 24 hours, WannaCry had infected more than 230,000 computers in over 150 countries.

“From a technical point-of-view, it was not particularly sophisticated. In fact, it exploited a vulnerability that had been known for 91 days and that had already been patched by Microsoft.

“Even so, an estimated 1.3 billion endpoints were eventually infected. In the UK, the National Health Service – a major client for Sophos – had to cancel 20,000 appointments and operations due to the ransomware. Whether any lives were lost as a result of it will never be known, but what is known is that it crippled the country’s health service (The History of Cyber Security — Everything You Ever Wanted to Know, 2019).“
Scale and Size of the Cybersecurity Threat in the U.S. and Worldwide

The most telling illustration of the scale and size of the cybersecurity threat is provided by IBM in their 2020 report. Here are a few of the key elements (IBM X-Force Threat Intelligence Index, 2020):

- 8.5 billion records breached in 2019, giving attackers access to more stolen credentials. Securing credentials and access controls is more important than ever.
- 150,000 vulnerabilities disclosed to date. Patching vulnerabilities is still a problem for many organizations and cybercriminals know that.
- Ransomware attacks up 67% year-over-year in Q4 2019. Threat actors are innovating with new ransomware code for destructive attacks.
- Operational technology (OT) attacks surged 2,000% year-over-year. Threat actors continue to shift their sights to attack vectors including IoT, OT and connected industrial and medical systems.
- Retail industry attacks increased. The number two industry after financial services, retail was targeted for payment card data and valuable loyalty program data.
- North America the biggest geographic target. Asia, Europe, the Middle East and South America trailed North America in number of attacks.

This amount of cyber threat activity has an increasingly alarming affect on every business sector, including the design and construction and built environment industry.

Wired Magazine noted in 2019 that numerous incidents had taken place but ransomware in particular was becoming an ever-growing threat. Significant cybersecurity incidents include:

- **Customs and Border Protection (CBP) Breach** in May 2019. The CBP breach involved both license-plate images as well as traveler ID photos that were stolen from a subcontractor working for CBP. Apparently, the unnamed contractor without CBP authorization downloaded and transferred the database including the breached images from federal government servers to their own company network. While CBP told the public that its own servers were unharmed by any cyberattack, it initially didn't reveal the full scope of the breach or specifics on what data was compromised.
However, there was commentary about what likely did get stolen: “…both the U.K. outlet The Register and Vice reported finding scores of traveler data on the dark web in the hours after that breach, including financial information, photos, and location information….I would be cautious about assuming this data breach contains only photo data,” said Chad Loder, the CEO of Habitu8, a cybersecurity firm that trains other companies on security awareness. The full scope of the breach may be much larger than what CBP revealed in its original statement, he said. In recent years, CBP has asked travelers for fingerprints, facial data, and, recently, even social-media accounts. “If CBP’s contractor was targeted specifically, it’s unlikely that the attacker would have stopped with just photo data.”

- **Ransomware Attacks.** While hardly new, these are broadening beyond hospitals, small businesses, and governments. “A destructive strain called LockerGoga has specifically been victimizing industrial and manufacturing firms—at times forcing production plants to switch to manual control or exacting long-term damage in systems that control physical equipment.”

- **Supply Chain Attacks.** “In March (2019), following a research report from the threat intelligence firm Kaspersky, computer maker Asus disclosed a supply chain attack sometime in the second half of 2018 that had compromised the company’s Live Update tool to push malware to almost 1 million customers.”

- **American Medical Collection Agency (AMCA) Data Breach.** “The company discovered that it had been breached in March, and filings with the US Securities and Exchange Commission indicate that the intrusion on AMCA’s systems lasted from August 2018 through March 2019. The incident was first publicly reported at the beginning of June after the medical testing firm LabCorp said that 7.7 million of its customers had data exposed because of AMCA, and Quest Diagnostics said it had had records from 12 million patients exposed. AMCA said that the compromised information included first and last names, dates of birth, phone numbers, addresses, dates of medical services, health care providers, and data on balances due.”

- **First American Data Exposure.** Data was improperly stored at this real estate and title insurance firm. “Discovered in May by security journalist Brian Krebs, the incident exposed 885 million sensitive customer financial records going back to 2003. They were accessible to anyone on First American’s website. It isn’t known whether anyone actually found and stole..."
the information before the company locked it down, but it was extremely easy to grab. Social Security numbers, driver's license images, bank account numbers and statements, mortgage and tax documents, and wire transaction receipts from millions of Americans were all included in the trove (Newman, 2019).

Even the World Economic Forum has a Centre for Cybersecurity, acknowledging both the importance of digital connection to worldwide development, and the impact of cyber threats. It is worth reading the Centre for Cybersecurity’s mission in full:

The **Centre for Cybersecurity** was established by the World Economic Forum to shape the future of cybersecurity and digital trust. The Centre is leading the global response to address systemic cybersecurity challenges and improve digital trust, to defend innovation and protect institutions, businesses, and individuals. We bring together policy-makers and operational leaders from the highest levels around the world through ongoing collaborative action and partnership across our network comprising business, government, civil society, academic leaders and top cyber experts (Centre for Cybsersecurity).

The projects the World Economic Forum are working on include:

- **Future Series: Cybercrime 2025.** In a joint project between the World Economic Forum (WEF) and University of Oxford-Oxford Martin School, WEF this project recognizes that financially motivated cyberattacks are “among the the top five global risks in the world today.” “Recognizing that the world is challenged by the unprecedented technological change driven by the Fourth Industrial Revolution, the report highlights that technological innovations such as artificial intelligence (AI), next generation networks (5G), the internet of things (IoT), operation technology (OT), physical convergence and quantum computing present both tremendous opportunities and unprecedented threats.”

  Outcomes and deliverables for this project include a) a series of workshops, a set of insightful reports, and a comprehensive final report.

- **Incentivizing Secure and Responsible Innovation.** This project involves “examining a standard approach for investors to assess, monitor, and improve the cybersecurity of their target or portfolio investment companies in order to improve understanding of post-investment roles and responsibilities
of investors in monitoring and helping grow portfolio companies' cybersecurity capabilities.”

“The investment community needs parameters and viable benchmarks to evaluate whether a company and its practices are cyber secure.”

**Profile of Cybersecurity Today**

Even an overview of the publications covering design and construction demonstrate a profile of a growing cybersecurity landscape and the threats that impact it.

The various articles published and topics tracked on the New York Times’ cybersecurity site illustrate the enormous variety of the problem (The New York Times Cybersecurity):

- Manufacturers Remain Slow to Recognize Cybersecurity Risks
- The Mad Dash to Find a Cybersecurity Force
- Learning to Attack the Cyberattackers Can’t Happen Fast Enough

McKinsey Digital has an extensive practice and resources for cybersecurity. (McKinsey Digital Cybersecurity). They “…believe cybersecurity should be an enabler of, rather than a barrier to, capturing and extending value in the digital economy. Our experienced, highly skilled experts help organizations measure their digital resilience, identify and prioritize critical assets for protection and investment, build leadership capabilities to neutralize threats, and make cybersecurity build-or-buy decisions.” Their activities include:

- Digital-Security Transformation
- Crisis Preparedness and Response
- Navigation of Cybersecurity Markets

Perhaps most relevant to the discussion in this course is McKinsey’s focus on adapting infrastructure to repel cyber threats. As they note in their report:

“The number and severity of cyber threats continue to grow exponentially as the world becomes increasingly connected. According to recent estimates from the research firm Gartner, by 2020 there will be 20.4 billion internet-connected devices, and approximately 37 percent of these will be used outside consumer settings—including large numbers dedicated to infrastructure monitoring and
control. While the proliferation of connected devices has created unprecedented productivity and efficiency gains, it has also exposed previously unreachable infrastructure systems to attack from a range of malicious groups with varying motivations (Critical resilience: Adapting infrastructure to repel cyberthreats, 2019)."

McKinsey’s major point is that it is necessary to build a cyberdefense infrastructure and, in their words, “an integrated defense is the only defense.” They also warn that everyone should start with the assumption that a cyberincident will occur. They have three key recommendations:

- Recruit new talent
- Form a cyber response team
- Cultivate a mind-set shift across the organization

Engineering News Record (ENR) has produced numerous articles as well as highly informative webinars about cybersecurity, available at https://www.enr.com/keywords/Cybersecurity (ENR Cybersecurity Articles). One compelling article, “Construction Cybercrime Is On the Rise” offers commentary by Phil Weaver of Warfel Construction and John G. Voeller of Black & Veatch which paints a grim picture of the preparedness of the construction industry for cybersecurity threats:

“Phil Weaver, senior director of IT at Warfel Construction, a construction firm with 230 employees and $235 million in revenue based in East Petersburg, Pa., thinks the industry is unprepared. ‘I don’t think GC’s and CM’s are worried enough about the impact a cyber incident can have,’ he says. ‘I think there is just a lack of understanding or realization that it can happen to us.’

“John G. Voeller, retired senior vice president, chief technology officer and chief knowledge officer for Black & Veatch, has a very big picture view, having been drafted over the years by think tanks and the government to help scope risk to critical infrastructure. And from where he sits, the view is bleak.

“ ‘Some construction executives are worried, but too large a number of them do not understand the situation well enough, and their risk managers are too often not technical enough, or connected to their [chief security officer] strongly enough, to really see how many holes there are in their dike—and how few thumbs they have that are effective,’ Voeller says. ‘They do not realize how precarious their situation is (Sawyer & Rubenstone, 2019).’ ”
While the article is worth a complete and thorough reading (see: https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise), the conclusion by Weaver, as well as Everardo Villasenor, construction IT leader and chief information security officer at DPR, is particularly alarming and compelling:

“… on a scale of 1 to 10, (Villasenor) gives the industry as a whole dismal marks. ‘[Construction’s] cybersecurity score is low, perhaps 3 on a 10-point scale,’ he says. ‘Many firms see cybersecurity as slowing operations or a high overhead cost versus perceived return on investment. Unfortunately, it has taken serious incidents for firms to truly understand the threat.’

“Warfel’s IT director Weaver was even less sanguine. ‘Two,’ he says. ‘I think it’s worse than most people know.’ ”

Redshift by Autodesk provides some advice for the construction industry. Author Joshua Glazer notes that in 2016, Construction Dive reported a 400% increase in ransomware attacks in the construction industry; in response, he created a list of five things to do:

- Don’t Let Your Receptionist Be Too Nice. “Make security a priority and provide Internet-safety training just like you provide job-site-safety training.”
- Don’t Skimp on Your Email System. “…cloud-storage solutions with strong security features turned on—such as two-factor authentication—are the way to go. Cloud-based companies are monitoring and protecting their systems from millions of users.”
- Consider Hiring an In-House Security Expert. ”...failing to secure your data can result in losses that could bankrupt your company—and even result in criminal complaints by the FTC.”
- Limit the Number of Admins. “…giving too many employees admin-level access… can become especially problematic, as networked systems like BIM grant access to your intellectual property remotely and throughout many third-party stakeholders.”
- Always Update Your Software. “Cybersecurity is an ever-evolving threat, and new technology (such as IoT sensors and smart locks) will introduce new security issues. It’s crucial that whatever software you use, you regularly update it to ensure the latest security holes are patched (Glazer, 2017).”
Victor Insurance has a 21 page slide deck that gives a comprehensive overview of the threat landscape for design firms (and construction); it’s definitely worth a thorough review. Their advice, echoing others, is (Coughline & Ackerman, 2019):

- Perform risk assessments to understand the data within your organization and safeguards to protect the security of that data
- Prepare and enforce data security policies and procedures
- Prepare and test Incident Response Plan
- Ensure experience on the Incident Response Team
- Document your due care measures (training and enforcement) being taken
- Insure yourself with appropriate coverage at appropriate limits
- Understand contractual obligations
- Execute service level agreements
- Repeat

**Information Technologies (IT) and Cybersecurity**

The term information technology (IT) is well known, referring to “The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information,” per Lexico (Meaning of information technology in English, 2020).

Cybersecurity or information technology security:

“…is a field within information technology involving the protection of computer systems and the prevention of unauthorized use or changes or access of electronic data. It deals with the protection of software, hardware, networks and its information. Due to the heavy reliance on computers in the modern industry that store and transmit an abundance of confidential information about people, cyber security is a critical function and needed insurance of many businesses. It also protects computer systems from theft or damage (Introduction to Information Technology/Cybersecurity, 2020).”

With office functions (email, customer relationships management, financial), project collaboration tools, and building information modeling (BIM) tools, most of the typical cybersecurity case studies and recommendations in this course revolve around IT. However OT, as described below and as further elucidated in the “Game Changing Innovations” chapter, is becoming more and more relevant and significant for the practicing architect, engineering, consultant, constructor, facility manager, or owner/client.
Operational Technologies (OT) and Cybersecurity

Operational Technology (OT) is defined as "the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc." (Wikipedia). More succinctly, OT is the utilization of computers to monitor or alter the physical state of a system. Also known as industrial control systems (ICS), OT is technically and functionally different than traditional IT systems.

Michael Chipley PhD, PMP, LEED AP, an important expert in the field of cybersecurity as it relates to OT, provides an excellent introductory resource via the Whole Building Design Guide (WBDG), a project of the National Institute of Building Sciences (NIBS). He defines ICS/OT systems as:

“…physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements.”

Chipley describes the key components of ICS as both building environmental controls (HVAC, lighting, etc.) and broader, more extensive and pervasive, systems such as the electrical power grid. He notes that there is an increasing tendency for ICS components and systems to be interconnected and internet enabled. These ICS systems can then be, if not fully protected, vulnerable entry points into an organization’s IT systems.

Chipley cites specific examples of malware that were focused on operational technologies and industrial control systems:

- Stuxnet
- Duqu
- Flame
- Shamoon

Stuxnet was a piece of malware that actually did physical damage to critical infrastructure:
“Stuxnet 'spoofed' the integrity of the uranium centrifuges and caused the centrifuges to overspin and self-destruct, while the operators console showed the system was operating within normal parameters.”

The Flame malware is particularly relevant to design and construction professionals:

“The Flame malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity, and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices.”

Based on the extensive threat and seriousness of these cyber attacks, the federal government has taken action to protect the critical infrastructure.

“In February 2013, Executive Order Improving Critical Infrastructure Cybersecurity was issued which requires the National Institute of Standards and Technology (NIST) to 'lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible.' ”

Within the article, Chipley addresses the ICS/OT in the context of:

- Communications Network and Business Systems
- Building Management System (BMS)
- Building Automation System (BAS) / Building Control System (BCS)
- Electronic Security System (ESS)
- Fire and Life Safety System (FLS)
- Power over Ethernet
- Smart Buildings / Intelligent Buildings

An emerging categorization of systems (like smart buildings) in which physical components (OT) and computational components (IT) interact is referred to by Chipley as cyber-physical systems. The technologies that this categorization refers to include:
• Internet of Things (IoT)
• Industrial Internet
• Smart Cities
• Smart Grid
• “Smart” Anything (e.g. Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances) (Chipley, 2020)

Putting this discussion into a historical framework, Figure 2 (Cyber-Physical Security Time Line Context. Credit: NIST Shyam Sunder Industrial Internet Workshop, March 2013) illustrates how physical systems, cyber systems and cyber-physical systems have evolved over time:

![Figure 2](image.png)

**IT versus OT**

It is important to elucidate the distinctions between IT and OT so that we can understand the factors at play as both relate to cybersecurity and the construction industry.

In Figure 3 (IT vs. OT Systems Comparison. Image courtesy of NIBS and WBDG), Michael Chipley provides a table comparing the features distinguishing OT and IT.
Chipley notes the relatively recent attention that OT has garnered, compared to IT:

“While federal agencies have been required to meet stringent Cybersecurity standards for the traditional IT systems since the Federal Information Security Management Act (FISMA) was passed in 2002, the same level of protection and analysis is just beginning to be developed for building control systems. Buildings are becoming increasingly reliant on technologies that allow centralized monitoring and control of multiple building systems (Building Automation, Fire and Life Safety, Energy Management, Physical Security, Access Control, etc.), to assist in accomplishing design and operational goals. Because of the unique operating and configuration of building control systems, traditional IT processes such as continuous monitoring, host based scanning, and automated patch management can cause building control systems to fail or become non-operational (Chipley, 2020).”

This evolution toward cyber-physical systems will become even more pronounced and significant as newer technologies emerge affecting the design profession, the construction industry, and the entire built environment.

**Game-Changing Technology | Innovation in Cybersecurity**

Chapter III will delve more deeply into various game changing innovations and their impact on cybersecurity but, suffice it to say, the effects will be enormous. Deloitte, for example, has developed a framework to discuss the chronic shortage of
cybersecurity talent, especially as new and emerging technologies change the threat landscape (Deloitte TFSA Toronto Financial Services Alliance).

New bandwidth capabilities such as 5G will require new approaches to cybersecurity, according to The Brookings Institution:

“5G will be a physical overhaul of our essential networks that will have decades-long impact. Because 5G is the conversion to a mostly all-software network, future upgrades will be software updates much like the current upgrades to your smartphone. Because of the cyber vulnerabilities of software, the tougher part of the real 5G “race” is to retool how we secure the most important network of the 21st century and the ecosystem of devices and applications that sprout from that network.”

The Brookings report noted that a 2017 malware attack caused financial devastation, and emphasized that it took place over a network not yet enabled with the advanced capabilities of 5G:

“The NotPetya attack in 2017 caused $10 billion in corporate losses. The combined losses at Merck, Maersk, and FedEx alone exceeded $1 billion. 5G networks did not exist at that time, of course, but the attack illustrates the high cost of such incursions, and it pales in comparison to an attack that would result in human injury or loss of life (Wheeler & Simpson).”

Blockchain has been touted as a significant breakthrough innovation that will change the cybersecurity landscape. There has been huge investor interest, according to McKinsey & Company:

“One sign of blockchain’s perceived potential is the large investments being made. Venture-capital funding for blockchain startups reached $1 billion in 2017. IBM has invested more than $200 million in a blockchain-powered data-sharing solution for the Internet of Things, and Google has reportedly been working with blockchains since 2016. The financial industry spends around $1.7 billion annually on experimentation (Higginson, Nadeau, & Rajgopal, 2019).“

The technology is not without its detractors, however: McKinsey also notes that, despite over 100 blockchain use cases having been identified, there has been little to show for all of the development and investment.
We’ll return to the topic of game changing innovations in Chapter III. Also, a PDH Academy course is available that delves more deeply into game changing innovations (Hagan S. R.).

PDH Academy
Cybersecurity for Architects
CHAPTER REVIEW QUESTIONS

Construction Industry Perspective

on Cybersecurity

1. In addressing what is “cybersecurity”, the question arises what is a cyber threat? It is an activity on a system or network:
   a. Meant to improve connectivity.
   b. Increases bandwidth and breadth
   c. That is malicious attempting to collect, disrupt, deny degrade or destroy
   d. That is also an app on an iphone/ipad

2. Among the disturbing trends IBM reports in its Threat Intelligence Index of 2020 is:
   a. Social Media has increased.
   b. 8.5 billion records compromised in 2019.
   c. Fewer fans of Facebook.
   d. Happiness apps are declining in sales

3. Which of the following is NOT an example of tools used in cybersecurity:
   a. Passwords
   b. Firewalls
   c. Bullet journaling apps
   d. Encryption
4. In the discussion of IT versus OT, operational technology includes “physical assets” such as all but the following:
   a. Water
   b. Auto
   c. Word Documents
   d. Marine and Aviation

5. IT (operational technologies) include all but the following
   a. Electrical Grid
   b. ERP systems
   c. BIM
   d. Accounts and Billing

6. The history of cyber security includes one of the first known malware programs called:
   a. Laser Scanning
   b. Creeper
   c. Powerpoint
   d. Gmail
II. Construction Industry Perspective on Cybersecurity

Construction Industry Stakeholders

The significant impact cyber threats have had on the health care industry, as mentioned above, suggest that the construction industry is also at risk: the industry is huge and therefore a logical target for malfeasance. As noted by the Associated General Contractors of America (AGC):

"Construction is a major contributor to the U.S. economy. The industry has more than 680,000 employers with over 7 million employees and creates nearly $1.3 trillion worth of structures each year. Construction is one of the largest customers for manufacturing, mining and a variety of services (Simonson, Ken)."

Construction industry stakeholders, including architects, engineers, consultants, estimators, constructors, sub contractors, building product manufacturers, software technology vendors, insurance agents and brokers, building suppliers and owners, and developers are therefore all subject to potential cyber threats.

What are the dangers to stakeholders in the construction industry? There are many, as noted by iSqFT:

“As the construction industry becomes more connected through internet-connected solutions and remotely accessible systems such as Building Information Modeling (BIM), telematics and project management software it creates more opportunities for hackers to launch a cyberattack.

“Construction firms have access to a wealth of information that might be desirable to hackers. Intellectual property, proprietary assets, architectural drawings and specifications as well as corporate banking and financial accounts are all prime targets. Access to employee information such as full names, Social Security numbers and bank account data used for payroll are frequently targeted in spear phishing scams. Hackers often go after general contractors and subcontractors as a means to gain access to clients’ networks (Data Breaches, Cyber Security and the Construction Industry, 2016).”

The importance of cybersecurity measures for construction firms was highlighted in an interview with Johann Dettweiler, director of operations for Fairfax, Virginia-based compliance management firm TalaTek:
“It’s important to note that cybersecurity is important for everyone from Fortune 500 companies to individuals working in a home office. One of the main reasons organizations don’t consider cybersecurity is they tend to think of their data as something other than a company asset. Construction companies in particular have a lot of physical assets from materials to vehicles to personnel that something as non-substantive as data can easily be overlooked as an asset to protect.

“However, all data is an asset and should be protected. Whether it is the private data of an organization’s workforce, such as social security numbers or private human resources (HR) information or the company’s proprietary data, such as building plans or construction time frames, if this data were to be exploited, it could have serious legal and/or financial ramifications for an organization (Goodman, 2020).”

Specific cybersecurity case studies are described later in this course.

**Built Environment | Digital Transformation | Cybersecurity**

The construction industry and built environment have typical been seen as a laggard in terms of automation and digital transformation. Both the McKinsey Global Institute and the World Economic Forum have had major research initiatives addressing the construction industry, productivity and digital transformation.

In 2016, McKinsey noted that large capital projects typically take 20% longer to finish than originally scheduled and can exceed budget by up to 80%. The challenge:

“While the construction sector has been slow to adopt process and technology innovations, there is also a continuing challenge when it comes to fixing the basics. Project planning, for example, remains uncoordinated between the office and the field and is often done on paper. Contracts do not include incentives for risk sharing and innovation; performance management is inadequate, and supply-chain practices are still unsophisticated. The industry has not yet embraced new digital technologies that need up-front investment, even if the long-term benefits are significant (Agarwal, Chandrasekaran, & Sridhar, 2016).”

**Figure 4** (The Construction Industry is the Least Digitized. Image: McKinsey Imagining Construction’s Digital Future) illustrates the extent that construction lags all other sectors. Lack of investment in innovation (less than 1% versus 3-4% for auto and aerospace) as well as in information technology accounts for a lot of this.
Contributing to the poor innovation performance for construction is the increasingly complex building types expected, as well as rapid response requirements; since many projects are considered “unique and one of a kind,” very little can be done to scale up improved practices and technologies.

The construction industry is among the least digitized.

McKinsey Global Institute industry digitization index; 2015 or latest available data

<table>
<thead>
<tr>
<th>Sector</th>
<th>Assets</th>
<th>Usage</th>
<th>Labor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT²</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance and insurance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wholesale trade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced manufacturing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oil and gas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemicals and pharmaceuticals</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic goods manufacturing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mining</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real estate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation and warehousing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail trade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment and recreation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal and local services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hospitality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Construction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agriculture and hunting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4
McKinsey goes on to suggest that there are five trends that will shape the industry moving forward and could have significant positive impact:

- Higher-definition surveying and geolocation
- Next-generation 5-D building information modeling
- Digital collaboration and mobility
- The Internet of Things and advanced analytics
- Future-proof design and construction

More information is available in **Figure 5** (Five Trends Shaping Construction’s Digital Future. Image: McKinsey).
Similar to efforts at McKinsey, the World Economic Forum (WEF) recognized lagging indicators in the construction industry and, in 2015, established the Future of Construction Initiative as part of their “Shaping the Future of Cities, Infrastructure and Urban Services” platform (Shaping the Future of Cities, Infrastructure and Urban Services).

The phases of the WEF platform outlined below illustrated the efforts of innovation underway that are potentially (actually most likely) to be challenged by the accelerating issues of cybersecurity.

The phases of the initiative include:

- “In 2015-2016 (Phase 1), the initiative assessed the current state of Engineering & Construction (E&C) industry challenges and opportunities. It also developed an industry transformation framework outlining key change vectors on company, sector & government level, illustrated by leading examples

- “In 2016-2017 (Phase 2), the initiative detailed case studies of innovative large-scale projects and from pilot projects & start-ups. It also developed lessons learned on key success factors for the industry including policy recommendations

- “In 2017-2018 (Phase 3), the initiative developed comprehensive scenarios of the E&C industry future based on mega-trends, including impact on jobs, sustainability, technology (Building Information Modeling etc.) highlighting strategic implications for all stakeholders along the value chain

- “Upcoming in 2018-2021 (Phase 4), in collaboration between the Forum, Oxford University and other partners, the initiative will form a central platform to exchange best practices and ideas guiding the IU industry in its necessary transformation by scaling the engineering and construction ecosystem beyond the existing major players and include key disruptors, creating and implementing policy reform and system transformation (Future of Construction and Infrastructure)
But all of these global efforts are potentially running headlong into the challenges posed by cybersecurity threats. The World Economic Forum in 2020 emphasized key challenges that need to be addressed by world leaders, first by noting three important points:

- Cybersecurity must be built-in to every product and system.
- Achieving this will pose four challenges for business leaders.
- By overcoming them, we can create a truly protected digital world.

The four leadership challenges were:

1. Real-time information sharing. “The pace of the digital world continues to increase exponentially. To keep up, security professionals have to address threats and security weaknesses rapidly, before cybercriminals strike. Speed is fundamental to an effective cybersecurity strategy”

2. Widespread collaboration in cybersecurity. “Effective cybersecurity must be deeply and widely collaborative. Collaboration enables the good guys to create a hive mind, to learn rapidly, constantly expanding our competency and capacity.”

3. Creating and promoting a common vision for integrated cybersecurity. “Public and private sector leaders must commit to creating a common vision for integrated cybersecurity - something akin to NATO, which is based on clearly defined fundamental principles….This vision for integrated cybersecurity must be comprehensive and inclusive, anticipating the next actions of cybercriminals rather than solely reacting to them.”

4. Promoting the technology platform we need to make this work. “Cybersecurity was not part of the design of most of the world's current infrastructure. This must change.”

Author Ken Xie concludes with both an entreaty and a challenge:

“Given these four challenges, it is only once we have true integration, both across national and geographic borders, and also within our own businesses, that cybersecurity will achieve its full potential of creating a truly protected world.

“As leaders of important global organizations, members of the WEF and its Centre for Cybersecurity, and as an individual deeply aware of the...”
importance of this imperative, I believe that cybersecurity is a responsibility we must all take on (Xie, 2020)."

**Venture Capital | Startups: Investing in Cybersecurity**

The message from McKinsey, the World Economic Forum, and many other observers of trends in cybersecurity technology and business practice and formulation is that this is an industry ripe for innovation and investing.

CB Insights reports that investors are more willing than ever to support cybersecurity startups. The investment research firm noted that “Private companies are stepping up, backed by millions of dollars of funding, to help tackle today’s mounting cybersecurity challenges.” The year 2018, as an illustration, saw over 600 investment deals go to private cybersecurity companies, almost a 40% increase over 2015 (The Increasingly Crowded Cybersecurity Unicorn Club, 2019).

The most recent market map by CB Insights, compiled in 2017 and shown in **Figure 6** (Cybersecurity’s Next Step Market Map Image: CBInsights, 2017) illustrated over 80 companies utilizing artificial intelligence (AI) for cybersecurity, categorized into 9 areas of operation:

- Anti Fraud & Identity Management
- Mobile Security
- Predictive Intelligence
- Behavioral Analytics / Anomaly Detection
- Automated Security
- Cyber-Risk Management
- App Security
- IoT Security
- Deception Security.
From technology vendors and government standards entities to industry organizations, there are a significant number of organizations influencing cybersecurity in the construction industry.

Technology companies are driving innovation today around the world. It is worthwhile to get a sense of how they are contributing their resources and talents to the cybersecurity effort.

- Autodesk has many software tools, and perspectives on technologies that will enable and optimize them. In Autodesk’s Redshift article “6 Big Ideas Show the Promise of Innovation in Infrastructure” (Smith, 2018) several important innovations are listed and explained:

1. Infrastructure Innovators Use VR Games to Streamline Scandinavian Tunnel Design.
2. Where New York Stands on 5 Big Infrastructure Projects

3. Water Infrastructure: Today’s Funding for Tomorrow’s Needs

4. How US Cities Can Finance Resilient and Equitable Infrastructure

5. Smart Cities Collaborative Tackles Transit Issues

6. To Save Our Infrastructure, Make Every Road a Toll Road

In addition, as mentioned in Chapter I.D above, Autodesk provides articles and advice for firms and individual professionals.

- Bentley Systems has developed reality modeling software termed “context capture” (Context Capture: Create 3D models from simple photographs, 2018), which allows design professionals and others to produce complex and interactive 3D models of urban conditions simply.

Bentley also helped Helsinki, the capital of Finland, develop “Helsinki 3D+” which is touted as a “new generation of city models.” Helsinki invested EUR 1 million to develop a 3D representation of the entire city with focus on a base data for smart city development. The intention was that this would be a platform on top of which open data and further input from business and technology companies would improve citizen and government services. The new platform could also be used by higher education, both for learning and professional development (City of Helsinki: Helsinki 3D+, 2018).

Bentley has taken a serious approach to cybersecurity. They chose Microsoft Azure and Altert Logic as their platform, but the mindset they exhibited was more important than the specific product. “Bentley Systems chose to focus on ISO 27001 compliance. As a company that operates around the world, they felt it was important to use a benchmark that is recognized globally and that is managed by an objective third-party rather than a specific country or vendor. ISO 27001 requires security controls like intrusion detection, vulnerability assessments, and real-time log collection and management (Bradley, 2019).”

- Trimble Inc. is a $3.1 billion global services company which focuses on many industries, but particularly building and construction as well as surveying. Founded as Trimble Navigation in 1978, it now has over 8,388 employees and includes many service, software and hardware products utilized in construction.
It also acquired SketchUp software in 2012 to complete an office-to-field platform for design and construction (Trimble).

Trimble emphasizes cybersecurity for construction. They cite Bryce Austin, principal of TCE Strategy and cybersecurity expert, who mentions three threats to be aware of: 1) Ransomware, 2) Phishing, and 3) Wire Transfers. As a commentary on the current state of preparedness of the construction industry:

“In the construction industry, I don’t see as many companies taking advantage of cybersecurity expertise or seeking outside training or help,” Austin said. “I’d like to encourage companies to consider having a cybersecurity coach and a technology coach to be successful in this space because it is a complex, ever-changing landscape.”

For those hoping to enact safeguards against cyber threats, they provide four keys:

- Deploy Multifactor Authentication
- Demand Strong Usernames and Passwords
- Backup Files
- Provide Consistent Training and Updates (Holtmann, 2019)

- The National Institute of Standards and Technology (NIST) is a world-class research and standards organization, with scientists there achieving three Nobel Prizes since 2005. NIST’s Building and Fire Research Lab focuses on the construction industry, and its Information Technology lab has the lead on cybersecurity. NIST publishes some of most important documents for the construction industry, and their cybersecurity website includes these critical initiatives and resources:
  - Computer Security Resource Center
  - Cybersecurity Framework
  - National Cybersecurity Center of Excellence
  - National Initiative for Cybersecurity Education (NICE)
  - Privacy Framework

Per their cybersecurity website:
“The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation. NIST’s cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country’s ability to address current and future computer and information security challenges (Cybersecurity).”

• The National Institute of Building Sciences (NIBS) is a unique organization in the construction industry:

“The National Institute of Building Sciences was established by the U.S. Congress in the Housing and Community Development Act of 1974, Public Law 93-383. NIBS is an authoritative voice that supports advances in building science and technology to improve the built environment.

“Congress recognized the need for an organization to serve as an interface between government and the private sector – one that brings together local, state, and federal representatives, the professions, industry, and labor and consumer interests to identify and resolve problems that hamper the construction of safe and affordable housing and commercial structures. NIBS is a resource to those who plan, design, procure, construct, use, operate, maintain, renovate, and retire physical facilities (About NIBS).”

One of NIBS’s projects is the Whole Building Design Guide (WBDG), whose section on Cybersecurity, authored by Michael Chipley, was noted earlier in this course. The critical importance of NIBS is that it works to convene both public sector and private sector entities to solve problems, and can thus have a unique impact on the construction industry with respect to cybersecurity.

• Victor Insurance, via the AIA Trust, provides an invaluable resource to architects and the entire construction industry with its Risk Management Guide. Victor’s conclusions are important:

“Although dealing with risks such as professional liability, client expectations and solving difficult design issues are often easier to address, more interesting, or may be more top-of-the-mind for every architectural firm, reminding yourself that you are a business and are not immune to the risks of technology and cyber crime is a great first step to addressing these risks proactively (An Architect’s Guide to Managing Cyber Threats).”
While not directly relevant to this course, another publication highlighted by Victor in their focus on risk on the AIA Trust website, “An Architect’s Guide to Buying Cyber Liability Coverage (Insurance Buyers' Council, Inc.),” may also be worth your time.

- The Associated General Contractors of America (AGC) provide professional educational resources on cybersecurity, including current and informative webinars (WebEd: Cybersecurity–New Mandatory Requirements for Defense Contractors, 2019).
Construction Industry Perspective

on Cybersecurity

7. The construction industry by virtue of its size and importance is subject to malfeasance by cybersecurity criminals. The scale of the industry, according to the AGC Chief Economist Ken Simonson, is all of the following EXCEPT:
   a. Is a major contributor to the U.S. economy
   b. Creates nearly $1.3 trillion worth of structures annually
   c. Employs fewer than a million people
   d. Consists of more than 680,000 employers.

8. Danger to the construction industry posed by cybersecurity threats include:
   a. Increased cable tv viewing
   b. Access to payroll data, including social security numbers and bank account data
   c. More sustainable construction
   d. Fewer schools construction

9. Digital transformation has been slow to take hold in the construction industry because of all except the following:
   a. Construction contracts do not provide for risk sharing and innovation
   b. Industry stakeholders have been slow to fix the basics.
   c. Project planning is uncoordinated between home office and field office.
   d. Construction sites are always perfectly clean

10. In terms of productivity and digitalization, construction lags all industries except
    a. Media
    b. Utilities
    c. Agriculture and hunting
    d. Retail trade
11. McKinsey suggests trends shaping the construction industry moving forward are all the follow, EXCEPT:
   a. Next-generation 5-D building information modeling
   b. Ink on vellum drawing
   c. Digital collaboration and mobility
   d. The Internet of Things

12. The World Economic Forum has plans to shape the Future of all of the following, EXCEPT:
   a. Infrastructure
   b. Cities
   c. Baseball stadiums
   d. Urban Services
III. Game Changing Innovation Impacting the Future of Cybersecurity

One of the most important developments in the advancement of design and construction is the emergence of game changing innovative technologies. From artificial intelligence (AI) to building information modeling (BIM) to digital twins and the sensor web, all of these technologies have become a major driver for both innovation and disruption. They also have implications for cybersecurity.

**Artificial Intelligence (AI) and Machine Learning (ML)**

Making significant inroads in both design and construction, artificial intelligence (AI) can help with analysis of issues for cybersecurity. For example, Autodesk is making use of AI and ML in conjunction with its BIM 360 software: “Construction IQ, formerly Project IQ, uses machine-learning algorithms to spot safety hazards and risk issues on Autodesk BIM 360 projects.

“The construction industry is already able to amass a massive amount of data,” says Patricia Keaney, director of Autodesk’s BIM 360 enterprise products. ‘There is so much data now people haven’t been able to fully consume or utilize it.’

“Autodesk is building a machine-learning tool, now called Construction IQ, to tackle this information overload, and have been testing it out with a few pilot customers over the last two years. The algorithm can comb through millions of data points in a BIM 360 project environment to unearth important trends and highlight unnoticed problems. ‘We can help customer find the signal in all that noise and surface what they should be focusing on for that data,’ says Keaney (Rubenstone, 2019).” See Figure 7 (“Construction IQ,” formerly Project IQ, uses machine-learning algorithms to spot safety hazards and risk issues on Autodesk BIM 360 projects.” Image and quote courtesy of Autodesk), below.

So how is this related to cybersecurity? As more and more innovation is occurring around the use of data and analytics, the incredible power of computing will not only assist in design and construction, as illustrated in the BIM 360 case above, but also in detecting anomalies that might occur with cyber intrusions.

AI combined with cybersecurity tools can enforce the integrity of the design and construction as it moves to more digital platforms. As Adam Janofsky of the Wall
Street Journal notes, cyber protectors are “…using machine learning to sort through millions of malware files, searching for common characteristics that will help them identify new attacks. They’re analyzing people’s voices, fingerprints and typing styles to make sure that only authorized users get into their systems. And they’re hunting for clues to figure out who launched cyberattacks—and make sure they can’t do it again (Janofsky, 2018).”

Figure 7
Big data and cheap computing also enabled the explosion of AI code that learns in software applications supporting every aspect of life. Add enabling tools like robotics, drones, and autonomous vehicles, as shown in Figure 8 (Artificial Intelligence, Machine Learning and other Emerging Computer Applications. Image: Forbes), and you have a world of cyber protection tools.
Augmented Reality (AR) / Virtual Reality (VR)

Just as AR and VR have taken off in terms of immersive technologies for the design and construction industry, so they potentially have a place in the cybersecurity toolkit.

In design and construction, AR is enabling full 3D visualization from the architecture office to the construction site. Matterport, a “reality-capture” camera manufacturer, is broadening the concept of AR for construction to include design tools, VR and eventually “full augmented reality” viewing:

“Broadening how models can be visualized is one area Matterport is exploring. Its 3D models can be exported to the GearVR and Google Cardboard virtual reality viewing platforms, a current feature it will continue to offer for free.

“But VR viewing is only one step toward the goal of creating augmented reality tools, says Bob Shakib, Matterport’s vice president for strategic partnerships. He says having the 3D model already built is ‘very convenient’ for authoring AR content because, unlike other AR creation systems that have an AR rendering engine but have to begin the AR creation process by mapping out the space, Matterport’s starting point is a fully photographed 3D model (Rubenstone, 2018).”

Similar to using AR/VR for design and construction, cybersecurity professionals are taking that same powerful visualization approach to understand how to defend against and prevent cyberattacks:

“How exactly does AR training work? First, let’s break down what AR is in a broader sense. AR allows the user to see the real world with virtual objects superimposed or composited with their reality. Essentially, users can interact with on-screen digital objects within the scope of the physical world they see on a daily basis.

“Companies like Inspired eLearning have made it their mission to provide training around security, cybersecurity and compliance with the help of VR (McClurg, 2019).”
So there is a convergence of the real and the virtual that can potentially dramatically improve cyberdefenses.

**Blockchain**

Blockchain is another innovation that has potential to transform both the construction industry and cybersecurity.

For construction, blockchain could be a game changer, according to PlanGrid’s Construction Productivity Blog. First let’s define what blockchain is:

> “Simply put, it’s broadly defined as a system that tracks transactions across a peer-to-peer network. In some situations, these transactions are made via either cryptocurrency or bitcoin. Blockchains acts as a distributed digital ledger among this peer-to-peer network where various kinds of agreements, whether they are financial transactions or contracts, can be recorded and confirmed once complete.”

Since blockchain is essentially designed to keep digital records continuously updated, for construction there could be four possible applications:

1. **Smart contracts.** “Smart contracts are largely hailed as the future of the construction industry. According to the University of West England, automated contracts that reduce the necessity of intermediaries and can save time and money are poised to make their mark on the industry.”

2. **BIM.** “When combined, BIM and blockchain can work to greatly enhance the effectiveness of smart contracts. For example, in BIM, the model itself can be used as part of the contract between the parties involved in the job. Therefore, all the parties would be working to match the actual physical construction on the project to the BIM model in the contract. Any deviation from the model may result in re-work or change orders. Incorporating BIM into smart contracts could also only award payment when the project is built according to the digital plans.

Combining BIM and blockchain, again, can work in holding all parties on a project accountable and creating a higher level of transparency. The combination could actually improve the effectiveness of BIM technology. Currently, BIM uses peer-to-peer networks for information sharing, but blockchain could make updates in real-time. This constant feedback and monitoring would help with transparency, lead to better overall
communication and ultimately result in a higher quality of workmanship on a project.”

3. Payments. “The blockchain concept is built around monetary exchange, albeit as it involves bitcoin and/or cryptocurrency. Meaning, blockchain can be utilized to streamline payment processing.”

4. Supply Chain Management. “Similarly, blockchain can help enable contractors to use unique digital-specific identifications to verify vendors and suppliers, and thereby grow their reputation over time based on how well their work is performed. These digital IDs can work two-fold, as they can also help your company verify the credentials of any subcontractors before they're ultimately hired (Ellis, 2019).”

Blockchain has such enormous potential that companies such as Trimble (Ramage, 2018), the Harvard Business Review (Tapscott & Viana Vargas, 2019) and even an organization called the Construction Blockchain Consortium (Welcome: HOW DISRUPTIVE TECHNOLOGIES ARE TRANSFORMING THE BUILT ENVIRONMENT) all have established stakeholds in the industry.

So where does cybersecurity fit in with blockchain? Forbes outlined how Blockchain can be utilized in cybersecurity (Arnold, 2018) with four promising use cases:

1. Decentralized Storage Solutions

2. IoT Security. “Hackers often gain access to systems by exploiting weaknesses in edge devices. These include routers and switches. Now, other devices such as smart thermostats, doorbells, even security cameras are also vulnerable. Simply put, the rigorousness is often not applied when ensuring whether these IoT devices are secure. Blockchain technology can be used to protect systems, and devices from attacks.”

3. Safer DNS (Domain Name Servers, or the internet addressing system).

4. Implementing Security in Private Messaging. “As conversational commerce becomes more popular, a lot of meta data is collected from customers during these exchanges on social media. While many messaging systems use end-to-end encryption, others are beginning to use blockchain to keep that information secure.”
Building Information Modeling (BIM)

Building information modeling (BIM) has potentially enormous cybersecurity implications. In an article related to construction sector in the U.K., Paul Lowe, a specialist construction sector solicitor, notes several key issues:

1. Problem Under-Reported. “…only 41% of even the most disruptive cyber security breaches are reported. This means that most cyber attacks in the construction sector may not become public knowledge, resulting in an untrue reflection of the scale and nature of cyber crime being presented.”

2. Cyber Security Not Prioritized. “…a leading survey indicates that the construction industry does not prioritise cyber security highly enough and the sector ought to educate itself in this vital area as the speed and extent of digitalisation accelerates.”

3. BIM as Major Trend. “One of the major trends in the construction world in recent years, particularly in the area of design, has been the introduction of building information modelling (BIM) – a way of digitally coordinating design data.”

4. Threats to Digital Data. “However, as BIM becomes more important, threats to the security of digital data become greater. In particular, BIM platforms are vulnerable to attack, manipulation, or other malicious activity by third party actors. The integrated nature of BIM also contributes to those threats. If designers and contractors are joining together a range of different designs and information from consultants who have different data, and this information is being pooled, the potential risk arises of malicious actors attacking one designer to affect the broader project.”

5. Not Just External Parties but also Internal Actors. “The risk not only lies with external parties but from internal actors too, who may wish to sabotage or otherwise detrimentally influence the course of a project. As information and designs from different individuals involved with a project are collected together, the consequence is that if one point of entry is compromised then a whole project can be accessed (Lowe, 2019).”
Internet of Things (IoT)

The Internet of Things (IoT) has enormous potential. As defined by Motley Fool, IoT refers to devices that are now connected to the internet, but generally didn’t have that capability earlier (Neiger, 2018). Although some remain skeptical as to its importance, the IoT is poised to deliver additional revenue to companies that capitalize on it, increasingly impacts vehicles, cities, and buildings and also has implications for cybersecurity.

According to author Richard Meyers (Meyers, 2017),

“…IoT devices provide local leaders with real-time data about community needs, and city managers use this information to create transformational solutions to make crowded cities more manageable and more affordable for everyone.”

Meyers also includes a good list of applications where IoT is being utilized. All of which could also have implications for cybersecurity:

- Street and traffic lights
- Transportation
- Parking
- Infrastructure and maintenance
- Waste management (including waste water)
- Air quality
- Crime
- Architecture
- Energy usage and distribution
- Traffic flow
- Pedestrian and bicycle needs

He concludes:

“The data alone will benefit nobody without a seamless system to analyze and aggregate the vast amount of information. An efficient messaging system will help take advantage of the new technology, and improve life experiences for residents and businesses while reducing costs for everyone involved.” It goes without saying that this seamless system integration will depend on a secure platform to be a success. Therefore, cybersecurity is essential to success.
Mobile Devices and APPs

Mobile computing and mobile APPs are exploding in number and popularity in support of construction. Perhaps the most important mobile computing device is the mobile phone, according to Procore: (Briggs, 2019)

“One piece of tech that has found a permanent place in the industry is mobile phones. Their sheer ubiquity make them a natural fit as a platform upon which to put apps and tools easily accessible for workers, and they’ve enabled the industry to “cut the cord” when it comes to communications. This has enabled decisions to get made faster and more efficiently, no longer relying on a wired on-site callbox or radio to speak to managers, and facilitates communication up and down the chain.”

These are also part of the growth in startup investment discussed below.

But the cybersecurity issues are critical and a potential roadblock to implementing this innovation. US-CERT (United States Emergency Readiness Team) has noted significant threats to mobile phones (Ruggiero & Fioote) and recommends actions to prevent and mitigate those threats.

Venture | Startup Innovations in Construct-tech

The venture research company CB Insights reports global equity funding in the construction industry or “construct-tech” sector as $778 million across 165 deals (Krishnan, 2016). Some of the top deals are highlighted in Figure 9 (Construction Tech Top Deals as of 11/28/2016. Image: CB Insights):
The number of investors involved in this surge of venture funding includes some of the most influential venture capital firms and private equity firms in the world. Figure 10 (Most Active Construction tech Investors. Image: CB Insights) illustrates which companies these investors are interested in.

The categories of their investments include (https://www.cbinsights.com/research/top-construction-tech-startup-investors/, 2017):

- Design Tools (e.g. Onshape, Flux Factory, Sefaira)
- Project Management Software (e.g. PlanGrid, Fieldwire)
- Equipment Marketplaces (e.g. Yard Club, Getable)
- Robotics and Drones (Fastbrick Robotics, Reconstruct)

The most relevant issue with respect to all of this innovation is that regardless of the activity, to date there appears to be little movement relative to cybersecurity and these startups. That is an amazing opportunity for companies knowledgeable about construction and cybersecurity to partner with investors and startups to coordinate a secure solution at scale.
# Most Active Construction Tech Investors

Firms Ranked by Unique Construction Tech Investments, 2012 - 2016 YTD (11/28/16)

<table>
<thead>
<tr>
<th>Investor</th>
<th>Rank</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Accelerator</td>
<td>1</td>
<td>TraceAir Technologies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Buildcom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VanVista</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IMERCO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Buld</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SupplyHog</td>
</tr>
<tr>
<td>Y Combinator</td>
<td>2</td>
<td>Vernox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>InsiteVR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EquipmentShare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Buildcom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plangrid</td>
</tr>
<tr>
<td>Andreessen Horowitz</td>
<td>3</td>
<td>Yard Club</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flux Factory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Onshape</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Getable</td>
</tr>
<tr>
<td>Brick &amp; Mortar Ventures</td>
<td>3</td>
<td>ManufactOn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rhombix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zien</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Building Connected</td>
</tr>
<tr>
<td>Borealis Ventures</td>
<td>5</td>
<td>Flux Factory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fieldens</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NEWFORMA</td>
</tr>
</tbody>
</table>

![CB Insights Logo](image-url)

*Figure 10*
III. Game Changing Innovation
Impacting the Future of Cybersecurity

13. One of the game changing innovations, artificial intelligence, is influencing construction because:

a. Backhoes are expensive
b. Construction industry is already able to amass a massive amount of data
c. The housing bubble may be returning
d. Tools are available at Home Depot

14. Autodesk has created a machine-learning tool called____________ to tackle information overload

a. Wacom tablet
b. Iphone
c. Construction IQ
d. Sketch Up

15. Ensuring authorized users are accessing construction digital assets is becoming enabled by what technology:

a. Laser scanning
b. Construction excavation
c. Artificial Intelligence
d. Roofing

16. What do AR and VR stand for in construction innovation?

a. Always Renovation
b. Augmented Reality and Virtual Reality
c. Viable Rework
d. Automated Ratching
17. The acronym AR stands for:

a. Aerial Recovery  
b. Augmented Reality  
c. Automatic Retrieval  
d. American Renovation.

18. Other game changing innovations include all of the following EXCEPT:

a. Blockchain  
b. BIM  
c. Nintendo Switch  
d. Digital Twin
IV. Cybersecurity Case Studies in the Construction Industry

Analyses of case studies of cybersecurity breaches and incidents are at the heart of understanding where the construction industry is today and what can be done to prevent damage, both financially and reputationally. As described in the iSqFt blog, there have been several highly publicized cases of cyber threats in the industry, including Turner Construction, Whiting-Turner Contracting, Central Concrete Supply Company, and others.

**Turner Construction**

Headquartered in New York, Turner is one of the largest construction management firms in the U.S. with offices in 24 states. They were hit by a spear phishing scam in March 2016. This type of attack:

“…is an email scam targeted at a specific individual, business or organization. Hackers spoof the “From:” field in an email to make it appear to come from a trustworthy source, say from your CEO or CFO. Typical spear phishing scams include messages requesting personal information on employees such as names and Social Security number, corporate banking account information, or login credentials.”

In response, a Turner Construction employee mistakenly sent information about taxes and other personally identifiable information (PII) to a fraudulent email account. All employees of Turner in 2015 were affected by the breach.

**Whiting-Turner Contracting**

Another widely publicized data breach occurred in March 2016 as Baltimore-based Whiting-Turner Contracting was notified by an outside vendor who prepared employee W-2 and 1095 tax forms that the vendors system’s were experiencing suspicious activity. The effect was significant:

“Around the same time, employees of Whiting-Turner were reporting fraudulent tax filings being made in their names. In addition to employee information, it is also possible that personal information on children and beneficiaries of employees who received healthcare insurance coverage through Whiting-Turner was compromised. Whiting-Turner has 31 offices in 18 states and Washington, D.C.”
Central Concrete Supply Company and others

“Central Concrete Supply Company out of California, Century Fence out of Wisconsin, Trinity Solar and Foss Manufacturing which makes nonwoven textile products for a number of industries, including construction, were also recent victims of spear phishing scams this year involving employee W-2 tax information.”

A Steel Mill in Germany

Cyberattacks have also affected OT. In this case:

“A spear phishing attack… led to physical damage at a steel mill in Germany. Malware was downloaded onto a company computer that had access to the plant’s business network. From there, the hackers were able to gain access the production network where they compromised the control systems resulting in a blast furnace not being able to be properly shut down (Data Breaches, Cyber Security and the Construction Industry, 2016).”

Target and Fazio Mechanical

A cyberattack at Target Corporation was widely publicized as an example of a construction-industry related data breach. In 2013, Target had its security and payment system breached,

“….compromising 40 million credit and debit card numbers, along with 70 million addresses, phone numbers and other personal information. Target was made aware of this situation in mid-December when the U.S. Department of Justice informed the company that their system was being attacked. Target had received notifications prior to this date, but had failed to act.”

It turns out that it was an employee of Fazio Mechanical, an HVAC contractor, who had his credentials to the Target network compromised when he clicked on a malicious email and fell victim to a phishing scheme (Munoz, 2015).

Bird Construction

Email attacks by phishing aren’t the only type of cyber threats that the construction industry has experienced. A Canadian contractor, Bird Construction, was highlighted in January 2020 by Canadian media as a victim of ransomware. In this case, the incident involved the encryption of company files. According to a Bird Construction company spokesman, the files were quickly restored and there were no major impacts. However,
“...the issue raised red flags about national security interests because the contractor is a provider of construction services for major federal and provincial projects including defense facilities and police stations (Goodman, 2020).”

**U.S. Department of Defense**

By 2020, the breadth and depth of cyber attacks prompted the U.S. Department of Defense to launch a Cybersecurity Maturity Model certification program in January 2020, to help:

“...ensure contractors on government projects have the necessary cybersecurity practices in place to protect the controlled unclassified information (CUI) to which they are privy (Slowey, 2019).”
IV. Cybersecurity Case Studies in the Construction Industry

19. The Turner Construction case study involved what cyberthreat?

a. Review shop drawings for a project  
b. Spear Phishing  
c. Prefabrication  
d. Social Media

20. White-Turner’s cyber incident involved__________ by an outside vendor.

a. Too much data overload  
b. Fraudulent Tax Filings  
c. Employees playing online games  
d. Social happy hours

21. Actual physical damage caused by a cyber incident was a case study involving

a. Employee training  
b. Fishing expeditions  
c. A steel mill in Germany  
d. Legoland California

22. The Target Corporation cyber incident in 2013, which compromised over 40 million individuals personal data, was construction related because:

a. Drywall was being utilized on store construction  
b. An HVAC contractor had hisTarget network credentials compromised  
c. Fire alarms went off  
d. Doors and windows were broken into
23. Red flags were raised in a Canadian construction firm's cyber incident because

a. Cost Overruns
b. The contractor Bird Construction also is involved in federal and provincial projects involving defense facilities
c. Of Heavy winds
d. Projects are being delayed

24. U.S. Department of Defense, in response to numerous cyber attacks, established__________ to ensure contractors follow necessary cybersecurity practices.

a. An awards program
b. A Cybersecurity Maturity Model Certification Program
c. Employee exercise program
d. A Military pay raise.
V. Making Your Own Cybersecurity Execution Plan

BIM Execution Planning as a Role Model

In 2007, the Penn State University Computer Integrated Construction (CIC) Program, in conjunction with the Pankow Foundation, began work on BIM Execution Planning as a key factor in the success of BIM on projects. Figure 11 illustrates two planning guides (BIM Project Execution Guide and Planning Guide for Facility Owners (Image: CIC Website) that are the cornerstone of the Project Planning Guides.

The Penn State University College of Engineering website (BIM Planning) has evolved significantly and includes now the Project Execution Planning Guide, The BIM Planning Guide for Facility Owners, The Uses of BIM, and Using BIM in Construction publications. From the outset, there has been an emphasis on owners, as noted below:
“In 2011, the Charles Pankow Foundation, along with others, awarded the CIC research program a grant to begin the development of an Owner’s Guide to Building Information Modeling. During the research and creation of the very successful BIM Project Execution Planning Guide, the group determined there was a need to develop a guide for facility owners and operators that includes a procedure to develop a strategy for integrating BIM throughout their organization. This guide, developed primarily for facility owners, will focus on the decisions required to define their organization’s standard BIM processes and practices; design information integration strategies; and identify appropriate BIM contracting strategies.”

So what is a BIM Execution Planning Guide, and how might it apply to our discussion of cybersecurity? As the Guide continues to describe it:

“This Guide provides a structured procedure… for creating a BIM Project Execution Plan. The four steps within the procedure include:

1. Identify high value BIM uses during project planning, design, construction and operational phases
2. Design the BIM execution process by creating process maps
3. Define the BIM deliverables in the form of information exchanges
4. Develop the infrastructure in the form of contracts, communication procedures, technology and quality control to support the implementation

The following steps are proposed for a Cybersecurity Execution Plan:

1. Team Building: Either with a project team or within a firm, gather stakeholders and discuss the goals of the plan
2. Educate: Present a range of technologies such as the ones listed in this course. Discuss both concepts and case studies
3. Discuss how three or four of these technologies can be the initial focus for a project or for a firm’s digital and innovative transformation
4. Make a specific action plan, including goals, objectives, and tasks and a timetable to complete them
5. Iterate and get constant feedback
6. Award all participants a certificate as a Cybersecurity Game Changer!
YOUR Cybersecurity Execution Plan

Begin your plan next Monday! The content of this course can be helpful to refer to while crafting your plan:

- Review the Introduction and Overview for a sense of broad cybersecurity concepts, as well as the extent of activities in the U.S. and worldwide
- Write a brief history of your firm, project, or partnership. Who all of the key stakeholders? How might cybersecurity affect day to day operations?
- Identify the technology partners who will play a key role in implementing cybersecurity, and what that role might be
- Also identify two or three primary game changing technologies that you anticipate might become relevant to your cybersecurity
- Review the cybersecurity case studies to identify lessons learned and challenges to anticipate and overcome

Also, consider including the tips to prevent data breaches provided by ISqFt (Data Breaches, Cyber Security and the Construction Industry, 2016):

- Install security software on your company’s servers and computers that can provide real-time protection and automatically receives the most up-to-date malware definitions.
- Make sure your firewalls are enabled and updated regularly with security patches.
- Train employees on security policies and practices. Employees should be required to change their passwords every three months.
- If employees are using mobile devices to access your company’s network they should be equipped with hardware and software data encryption and passwords or PIN locks should be used.
- Secure your company’s Wi-Fi network, both at the office and at the jobsite, by encrypting your wireless signal, securing your router with a password and filter MAC addresses of devices so only employees and authorized personnel can access your network.
- Regularly backup data offsite or with a trusted cloud storage provider.
VI. Conclusion and Path Forward

This cybersecurity course has been a whirlwind review of the state of cybersecurity globally as well as locally. As we wrap things up, here are a few additional resources.

AIA Trust Recommended Security Essentials

The AIA Trust and Victor Inc. provides a series of recommendations for all professionals, based on information provided in IBM’s 2015 Cyber Security Intelligence Index: (An Architect’s Guide to Managing Cyber Threats):

1. Build a risk-aware culture

Whether you open a dubious attachment, click on an unknown link, use an infected flash drive, or fail to install a security patch on your laptop, everyone is at risk. Educate your employees about cyber risks and the measures that they can take to protect themselves and the company.

2. Manage and report all incidents

Report all cyber and other potential attacks. Security breaches that occur at different companies or different locations may be related, but this can only be discovered if incidents are reported and analyzed.

3. Defend the workplace

Ensure all devices connected to a network – from a laptop to a printer to a smart TV – are up to date with the latest security software and follow all cyber security management and policy enforcement.

4. Security by design

One of the biggest vulnerabilities in information systems – and wastes of money – comes from implementing services first and adding on security as an afterthought. Build security into your network from the beginning and maintain regular tests to track conformance and compliance.

5. Keep it clean

Cyber criminals target people and businesses that are using old, out of date software. Maintain a comprehensive security system and install necessary updates and patches as they are released.
6. Control network access

Companies that channel registered data through monitored access points will have a far easier time spotting and isolating malware.

7. Security in the clouds

If your company utilizes public cloud data centers, ensure you have the tools and procedures in place to monitor possible threats and isolate your data from other companies in that data center.

8. Patrol the neighborhood

Ensure your vendors and clients are also aware of your risk-aware culture.

9. Protect the company’s crown jewels

Every company has crown jewels, whether it is scientific data, acquisitions documents, or clients’ financial and personal information. Whenever your company carries out an inventory, critical data should get special treatment – guarded, tracked and encrypted as if the company’s survival depends on it.

10. Track who’s who

Ensure you have procedures in place to manage the access and permissions of your employees. If an employee leaves, you must have the control to revoke any access they have to company, client and vendor information.”

**Flipboard Magazine “Cybersecurity for Architects”**

Flipboard, a powerful visual interface to a news feed and collaboration tool, presents significant information on cybersecurity, smart cities, and the topics relevant to this course via the collection entitled “Cybersecurity for Architects” as seen in Figure 12 (Hagan S., 2020). Join and contribute to this resource at [Cybersecurity for Architects Flipboard Magazine](#).
COVID-19 Pandemic and Cybersecurity
As this course is being finalized, the COVID-19 Pandemic is raging globally and is already changing world-wide economies, social structures, and even the response to the built environment. The FlipBoard mentioned above and shown in Figure 12 has many references such as the following which illustrate how cyberscurety threats are actually increasing during the pandemic:

- “FBI says cybercrime reports quadrupled during COVID-19 pandemic” (Cimpanu, 2020)
- “Coronavirus: Why the pandemic is a hotbed for cyber attacks – CityAM” (Warrington, 2020)
- “Society's Dependence on the Internet: 5 Cyber Issues the Coronavirus Lays Bare” (Denardis & Daskal, 2020)

These issues citing COVID-19 and CyberSecurity will be continually tracked on the FlipBoard (again, for reference: Cybersecurity for Architects Flipboard Magazine).
VII. Final Thoughts

Architects and their professional practice involve people, places, and products. The people include professional colleagues, consultants, constructors, specifiers, owners/clients, and the general public. The places are the projects in planning, design, construction, commissioning, that ultimately become fully occupied and operational buildings. The products are components specified to perform as expected in the building and in the furnishings, fittings and equipments. All of these dimensions of architectural practice have the potential to be a challenge with respect to cybersecurity threats.

This course has meant to inform, educate, and inspire the architect to be ever vigilant, and add this knowledge and expertise to the toolbox of his or her professional trade. Well-informed architects can be leaders in cybersecurity.

A key to the future is to look to the past, understand the present, and envision the future. Keep informed, and stay cyber-protected!
Table of Figures

Figure 1 Infographic: OT vs. IT Cybersecurity (Image: Waterfall-security.com) ............ 15
Figure 2 Cyber-Physical Security Time Line Context (Credit: NIST Shyam Sunder
Industrial Internet Workshop, March 2013) ................................................................. 27
Figure 3 IT vs. OT Systems Comparison (Image: WBDG) ................................................ 28
Figure 4 The Construction Industry is the Least Digitized (Image: McKinsey Imagining
Construction’s Digital Future) ......................................................................................... 34
Figure 5 Five Trends Shaping Construction’s Digital Future (Image: McKinsey) .......... 35
Figure 6 Cybersecurity’s Next Step Market Map (Image: CBInsights, 2017).................. 39
Figure 7 "Construction IQ," formerly Project IQ, uses machine-learning algorithms to spot
safety hazards and risk issues on Autodesk BIM 360 projects." (Image and quote courtesy
of Autodesk) ..................................................................................................................... 47
Figure 8 Artificial Intelligence, Machine Learning and other Emerging Computer
Applications (Image: Forbes) ............................................................................................ 48
Figure 9 Construction Tech Top Deals as of 11/28/2016 (Image: CB Insights) .......... 55
Figure 10 Most Active Construction tech Investors (Image: CB Insights) .................... 56
Figure 11 BIM Project Execution Guide and Planning Guide for Facility Owners (Image:
CIC Website) ..................................................................................................................... 64
Figure 12 Cybersecurity for Architects (Image: FlipBoard Magazine) ......................... 69
VIII. Bibliography


Meaning of information technology in English. (2020, February 27). Retrieved February 27, 2020, from Lexico: https://www.lexico.com/definition/information_technology


Slowey, K. (2019, December 19). *DOD will start requiring contractors to meet cybersecurity standards next month*. Retrieved February 27, 2020, from


Xie, K. (2020, January 13). *Four key challenges for cybersecurity leaders.* Retrieved March 2, 2020, from World Economic forum: https://www.weforum.org/agenda/2020/01/four-key-challenges-for-cybersecurity-leaders/
IX. Chapter Review Questions and Evaluative Feedback

I. Introduction and Overview

1. In addressing what is “cybersecurity,” the question arises what is a cyber threat? It is an activity on a system or network

   a. Meant to improve connectivity. This is not true about cyber threats in that they often slow down or bring to crawl computer and cloud networks.
   b. Increases bandwidth and breadth. FALSE Typically cyber threats will REDUCE or eliminate bandwidth.
   c. That is malicious attempting to collect, disrupt, deny degrade or destroy. TRUE Cyber threats can be incredibly destructive as several of the case studies in this course illustrate.
   d. That is also an app on an iphone/ipad. FALSE. Cyberthreats are the result of bad actors and / malware or other computer viruses.

2. Among the disturbing trends IBM reports in its Threat Intelligence Index of 2020 is

   a. Social Media has increased. FALSE. If anything, social media has increased.
   b. 8.5 billion records compromised in 2019. TRUE. This is indicative of the enormity of the damage that cyber threats have caused.
   c. Fewer fans of Facebook. FALSE, if anything there are millions more fans of facebook, fake or authentic.
   d. Happiness apps are declining in sales. FALSE, But irrelevant to the topic.

3. Which of the following is NOT an example of tools used in cybersecurity

   a. Passwords. This IS a tool of cybersecurity
   b. Firewalls. This IS a tool of cybersecurity
   c. Bullet journaling apps. TRUE. This is not an example of cybersecurity tools.
   d. Encryption. This IS a tool of cybersecurity.
4. In the discussion of IT versus OT, operational technology includes “physical assets” such as all but the following:

   a. Water. This is a REAL asset  
   b. Auto. These are REAL physical assets.  
   c. **Word Documents.** TRUE. This is not an operational technology.  
   d. Marine and Aviation. These are examples of OT

5. IT (operational technologies) include all but the following

   a. **Electrical Grid.** This is NOT an example of IT, but rather OT.  
   b. ERP systems. This is IT  
   c. BIM. Building information modeling is a “virtual asset” and therefore IT.  
   d. Accounts and Billing. These are office software products that are IT.

6. The history of cyber security includes one of the first known malware programs called:

   a. Laser Scanning. This is a hardware and software tool, not malware  
   b. **Creeper. This Is correct.**  
   c. Powerpoint. This is a Microsoft Office product for presentations.  
   d. Gmail. This is a Google product for messaging.

**II. Construction Industry Perspective on Cybersecurity**

7. The construction industry by virtue of its size and importance is subject to malfeasance by cybersecurity criminals. The scale of the industry, according to the AGC Chief Economist Ken Simonson, is all of the following EXCEPT:

   a. Is a major contributor to the U.S. economy. This is not an exception but is correct.  
   b. Creates nearly $1.3 trillion worth of structures annually. This is not an exception but is correct.  
   c. **Employs fewer than a million people.** This IS an exception. Construction employs over 7 million people.  
   d. Consists of more than 680,000 employers. This is not an exception but is correct.
8. **Danger to the construction industry posed by cybersecurity threats include:**

   a. Increased cable TV viewing. This is not a danger
   b. *Access to payroll data, including social security numbers and bank account data.* This is correct and is a danger to the industry.
   c. More sustainable construction. This is a positive trend for both architects and the construction industry.
   d. Fewer schools construction. This is not correct and in fact school construction has been growing.

9. **Digital transformation has been slow to take hold in the construction industry because of all except the following:**

   a. Construction contracts do not provide for risk sharing and innovation. This is true and therefore not an exception to the statement.
   b. Industry stakeholders have been slow to fix the basics. This is true and therefore not an exception. The construction industry has a whole lags far behind other industries in investing in basic transformation and digitalization.
   c. Project planning is uncoordinated between home office and field office. This is true and not an exception.
   d. **Construction sites are always perfectly clean.** Construction sites are NOT often well organized so this statement is incorrect and an exception.

10. **In terms of productivity and digitalization, construction lags all industries except**

    a. Media. This is not an exception because media ranks high on digitalization.
    b. Utilities. This is not an exception
    c. **Agriculture and hunting.** Correct, according to McKinsey these two activities are less productive and digital than construction
    d. Retail trade. This is not an exception
11. McKinsey suggests trends shaping the construction industry moving forward are all the follow, EXCEPT:

a. Next-generation 5-D building information modeling. This is not an exception and IS a major trend moving forward.

b. **Ink on vellum drawing.** This is a very old and ancient drawing technique and NOT a trend moving forward

c. Digital collaboration and mobility. This is not an exception and IS a major trend moving forward.

d. The Internet of Things. This IS a major trend that could have significances for the PRODUCTS part of people places products in the industry.

12. The World Economic Forum has plans to shape the Future of all of the following, EXCEPT:

a. Infrastructure. WEF definitely is interested in infrastructure

b. Cities. WEF has the city as a major focus

c. **Baseball stadiums.** These are NOT on the radar of WEF

d. Urban Services. This is important to WEF

### III. Game Changing Innovation

*Impacting the Future of Cybersecurity*

13. One of the game changing innovations, artificial intelligence, is influencing construction because:

a. Backhoes are expensive. This answer is off track from the question

b. **Construction industry is already able to amass a massive amount of data.** This is exactly why construction needs AI.

c. The housing bubble may be returning. This is off track and not correct anyway.

d. Tools are available at Home Depot. This is not relevant to the topic of AI.

14. Autodesk has created a machine-learning tool called____________ to tackle information overload

a. Wacom tablet. This was NOT created by Autodesk.

b. Iphone. Apple created the iphone and ipad

c. **Construction IQ.** This IS correct, and is a major initiative for Autodesk moving forward

d. Sketch Up. This is a Trimble product.
15. Ensuring authorized users are accessing construction digital assets is becoming enabled by what technology:

a. Laser scanning. Not correct. This is used to develop 3D point clouds for construction and real estate.
b. Construction excavation. This is an analog activity not related to technology.
c. **Artificial Intelligence.** This is correct and is becoming an invaluable asset for the construction industry.
d. Roofing. This answer is not relevant to the topic of AI

16. What do AR and VR stand for in construction innovation?

b. **Augmented Reality and Virtual Reality.** Yes, that is what these initials stand for in the industry.
c. Viable Rework. Not a real answer
d. Automated Ratching. Nope

17. The acronym AR stands for:

b. **Augmented Reality (AR) allows the user to see the real world with virtual objects superimposed or composited with their reality.** Yes, and is becoming more and more relevant for both architecture construction and real estate.
c. Automatic Retrieval. Nope
d. American Renovation. Not a real answer

18. Other game changing innovations include all of the following EXCEPT:

a. Blockchain. Yes
b. BIM. Definitely is game changing and influential
c. **Nintendo Switch.** A gaming device and not really an innovation for this industry.
d. Digital Twin. Definitely making headway as an innovation.
IV. Cybersecurity Case Studies in the Construction Industry

19. The Turner Construction case study involved what cyberthreat?

a. Review shop drawings for a project. Not correct.
   b. **Spear Phishing.** A spear phishing scam in March 2016 occurred when a Turner Construction employee mistakenly sent information about taxes and other personally identifiable information (PII) to a fraudulent email account.
   c. Prefabrication. Not a relevant response to question.
   d. Social Media. This was not the case in this incident.

20. White-Turner’s cyber incident involved___________ by an outside vendor.

a. Too much data overload. Not correct
   b. **Fraudulent Tax Filings.** CORRECT. In addition to employee information, it is also possible that personal information on children and beneficiaries of employees who received healthcare insurance coverage through Whiting-Turner was compromised.
   c. Employees playing online games. Not in this case
   d. Social happy hours. Not really a case for cyber threat.

21. Actual physical damage caused by a cyber incident was a case study involving

   b. Fishing expeditions. Generally not a venue for cyber threats.
   c. **A steel mill in Germany.** Hackers were able to gain access the production network where they compromised the control systems resulting in a blast furnace not being able to be properly shut down.
   d. Legoland California. Not really relevant to cyber threats in construction.
22. The Target Corporation cyber incident in 2013, which compromised over 40 million individuals personal date, was construction related because:

a. Drywall was being utilized on store construction. Not an issue for cyber
b. An HVAC contractor had his Target network credentials compromised. Correct “….compromising 40 million credit and debit card numbers, along with 70 million addresses, phone numbers and other personal information

23. Red flags were raised in a Canadian construction firms cyber incident because

b. The contractor Bird Construction also is involved in federal and provincial projects involving defense facilities. YES

c. Of Heavy winds. Not a cyber factor.
d. Projects are being delayed. Not relevant to cyber.

24. U.S. Department of Defense, in response to numerous cyber attacks, established__________  to ensure contractors follow necessary cybersecurity practices.

a. An awards program. Not happening.
b. A Cybersecurity Maturity Model Certification Program. CORRECT
c. Employee exercise program. Not relevant to cyber.
d. A Military pay raise. Not associated with the statement.
X. Author Biography: Stephen R Hagan FAIA

Stephen R Hagan FAIA CCM is recognized as an industry expert on technology | innovation, real estate, and the construction marketplace.

In August 2012, Stephen retired from the federal government after 37 years and is now consulting about BIM, Innovation and Online Technologies. Steve is President | CEO of Hagan Technologies in Reston, VA. Stephen is currently a member of the AIA Documents Committee.

Stephen was program and project management lead for the U.S. General Services Administration PBS Project Information Portal (PIP) and a founding member of the GSA 3D / 4D Building Information Model (BIM) team.

The AIA TAP Innovation awards program, which Steve founded (as TAP BIM Awards) in 2003, in 2014 celebrated its 10th year and includes partnerships with COAA, IFMA, and the AGC BIM Forum. In 2015, this program celebrated 11 years as a leading example of innovation and technology foresight for the Institute. In 2012-13, Hagan Technologies partnered with Onuma Inc. on development of a Strategic Plan and 5 Year Road Map for the Space and Equipment Planning System (SEPS) and the world-wide facility management system (DMLSS-FM) for the Department of Defense (DoD) and Veterans Administration (VA).

In 2014, Hagan Technologies supported Onuma Inc with a new FED iFM initiative for the DoD Defense Health-care Administration (DHA) that broadly supported the entire FM community in the public sector and broadened to the entire Design, Construction, Facilities Management / Operations communities. In 2015, Hagan Technologies branched out to include strategy and support for online, social media and collaborative technologies for the global travel industry. In 2016, through engagement with Geo-Buiz, the Open Geospatial Consortium (OGC), and NIST’s Smart Cities program, Hagan Technologies now is focused on emerging and innovative technologies supporting Smart | Connected | Sustainable | Resilient Cities and Urban Eco-Districts.

In 2018 to 2020, Game Changing Innovation, Cybersecurity for Architects, and start-up initiatives in the global construction industry | built environment continue apace and A’20 AIA Los Angeles.