National Institute of BUILDING SCIENCES™

CYBER-PHYSICAL IMPACT MODELING WEBINAR

NOV 28, 2023 @ 1:00 PM – 2:00 PM ET

https://www.nibs.org/events/cyber-physical-impact-modeling-webinar

ACCREDITED BY:

AIA Learning Units: 1 LU

ICC CEU: 0.10 CEU

SPEAKERS

ARI REUBIN MODERATOR

SVP of KMC Consulting a division of KMC Controls, Inc.

EJ VON SCHAUMBURG

Co-CEO, Red Bison

FRED GORDY

Director, OT Risk Assessments at Michael Baker International

HON. LUCIAN NIEMEYER

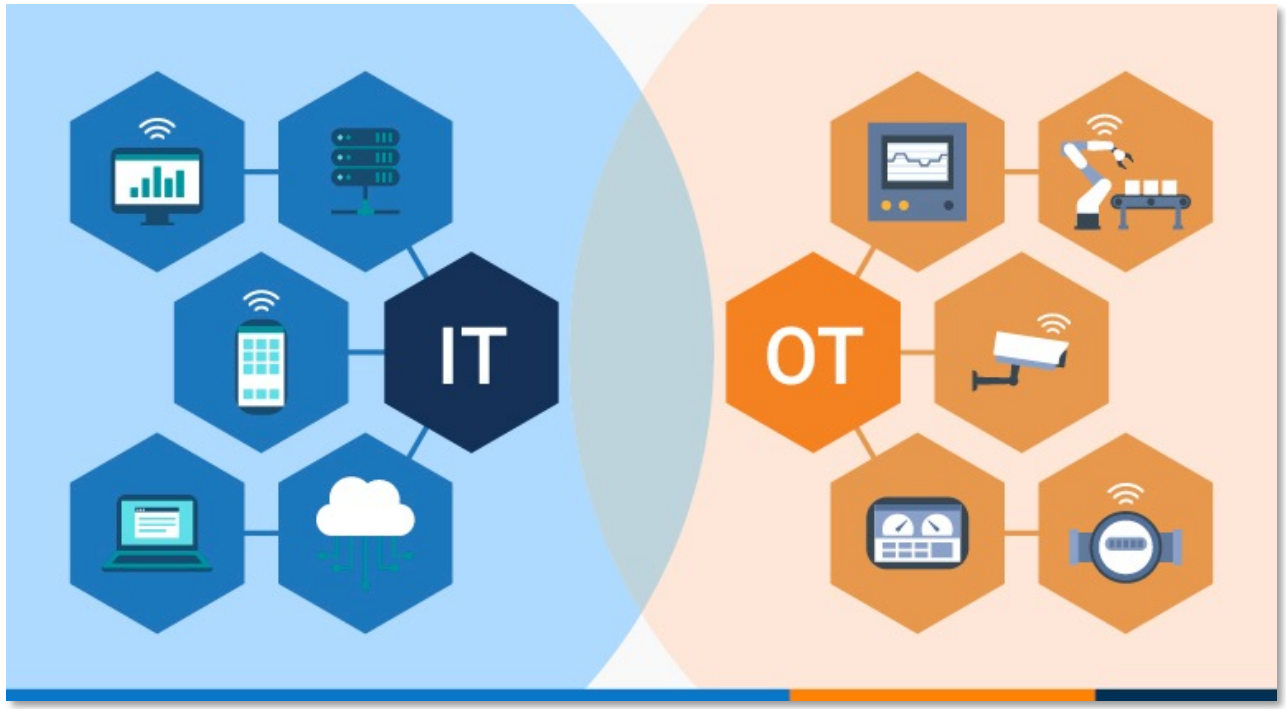
CEO & Chairman of Board of Directors, Building Cyber Security

ANDREW BALSTER

President, Physical Space Practice, Geniant

LEARNING OBJECTIVES

- ✓ Understand that the risk profile of current and emerging cyber threats to undermine the functional, operational, and safety needs of occupants and owners of commercial and institutional buildings cannot be overstated.
- ✓ Discover the need for a trusted cyber-physical framework for scoring the risk profile to protect building management systems and reduce risks to life, safety, and health for protection of employees and visitors.
- ✓ Gain understanding and access to implement a market-driven Cyber-Physical Framework (CPF) created by cyber-secure stakeholders to improve physical citizen security and safety.
- ✓ Understand that the strategic intent of this framework is to achieve the highest short- and long-term reduction of risk and cost that may be triggered by a disruption or adverse alteration to building operations, with the highest emphasis on hazard mitigation for personal injury, loss of life, and harm to the environment.



As technologies evolve, IT/OT convergence is giving business and/or property owners unprecedented flexibility, capabilities, and vulnerabilities.(1)

(1) https://www.onlogic.com/company/io-hub/it-vs-ot-how-information-technology-and-operational-technology-differ/).

BIGGEST CYBER SECURITY TRENDS IN 2024[3]

- ✓ More IoT devices talking to each other and accessing the internet means more potential "ins" for cyber attackers to take advantage of. For example, work-from-home risks by connecting or sharing data over improperly secured devices.
- ✓ As AI increases in sophistication, owners/operators may see smarter AI-powered attacks.
- ✓ Generative AI tools, such as *WormGPT* to enable more attackers to make smarter, more personalized approaches, and deepfake attacks to become increasingly prevalent.

- ✓ Zero trust moves from being a technical network security model to something adaptive and holistic, enabled by continuous AI-powered real-time authentication and activity monitoring.
- ✓ Cyber Warfare & State-Sponsored Cyber Attacks.
- ✓ Implementation of and compliance to Cyber-Physical Security (CPS) standards and frameworks. For example, BCS[4] framework to identify and assess the operational technology (OT) cyber risk - rooted in global industry standards, such as ISA62443[5]

(3) https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=685819255f13;
(4) https://buildingcybersecurity.org/
(5) https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

BUILDING
Cyber Security

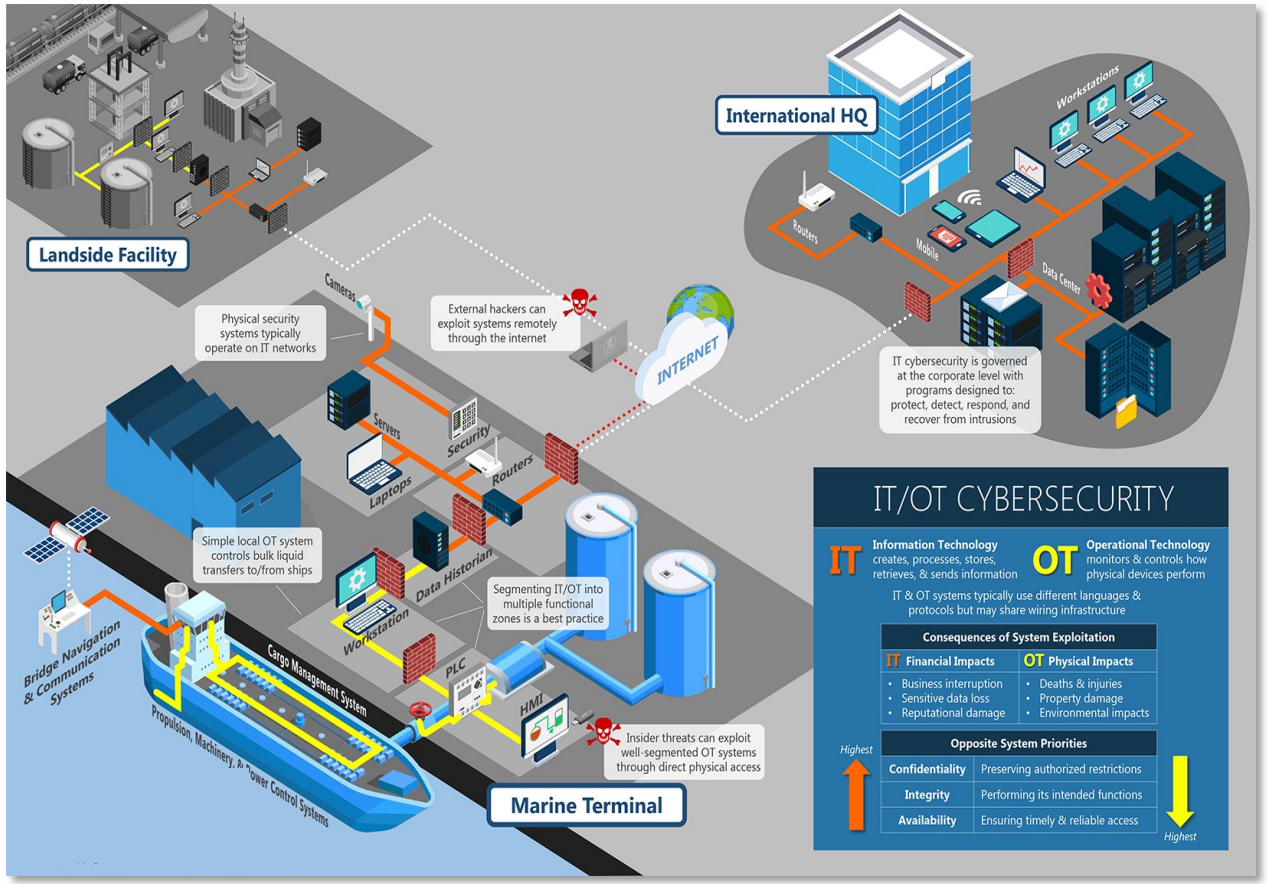
Addressing the Gap

Physical Cybersecurity & Operational Technology

A 501(c)(6) organization established on Feb 21, 2020

OT CYBERSECURITY THREAT LANDSCAPE IN 2023[(2)]: WHAT LEADERS FEAR & RISK DRIVERS

- ✓ Malicious attacks through connected devices, including via the Internet of Things **(40%)**
- ✓ Unauthorized access to sensitive data by malicious insiders **(29%)**
- ✓ Ransomware attacks **(23%)**
- ✓ Politically motivated attacks **(19%)**



- ✓ More than a third of respondents **(36%)** admit they still use Windows NT (an OS first released in 1993 and last supported nearly 20 years ago in 2004)
- ✓ Nearly half **(46%)** say they still use Windows XP (released in 2001), for which support ended almost nine years ago in 2014.
- ✓ Well over half **(57%)** utilize workstations running Windows 7, for which support expired three years ago. The same number **(57%)** depend on Windows 8, which Microsoft stopped supporting in Jan 2023.

(2) https://blogs.blackberry.com/en/2023/04/operational-technology-cyberattacks-and-2023-threat-landscape

THERE ARE MANY OT SYSTEMS

Fire Systems
- Fire Detection Systems (alarms)
- Fire Protection Systems (sprinklers)

HVAC Systems
- Ventilation, Chillers, Air Handling, Purification
- Air Quality, Health

People Transport Systems
- Elevators
- Escalators
- Moving walkways

Lighting Systems
- Standard lighting and shades
- Emergency lighting

Utility Systems
- Gas
- Water, Boilers, Filtration
- Electric (including Backup Generators, UPS, Solar, Wind)

Physical Access Systems
- Physical Security Control
- Video Surveillance
- People Count

A/V and Digital Signage
- Standard
- Emergency

Voice Communication Systems
- Standard
- Emergency

Voice Communications (wired & wireless)
- Parking Systems
- Access
- EV Charging

Building Automation Systems
- IT Systems
- Owner Network
- Property Management

Existing Frameworks

Proposed BCS	ISA/IES 62443	DoD Model	DoE Maturity (C2M2)	NIST Tier Model
BRONZE	Maturity 1	Basic	Level 0	Partial
SILVER	Maturity 2	Intermediate	Level 1	Risk Informed
GOLD	Maturity 3	Good	Level 2	Repeatable
PLATINUM	Maturity 4	Proactive	Level 3	Adaptive
		Advanced		

The BCS Cyber-Physical framework (https://buildingcybersecurity.org/) seeks to harmonize existing government frameworks and convert for private industry adoption.

Harmonize Frameworks and Incentivize Private Industry Adoption

Standards Consolidation

Consolidation of standards already in public domain

Dynamic Threat

Framework designed to provide value for entire system lifecycle due to evolving threat

Adaptive Model

Framework will evolve to meet changing threats

Recertification

Evolving threat environment requires on-going education

Assessment

Provide parameters for third party assessment of facilities based on framework scoring metrics

Tenant Rating

Public or private - Owner discretion

Value Proposition for Key Stakeholders

CRE OWNERS & OPERATORS

Options to choose security level of investment to meet stakeholder requirements

Clearly defined operating costs to meet insurance company discounts for assets under their control, as well as occupants

TECHNOLOGY COMPANIES

OT platforms with established baselines and committed service levels across industries

Product and technology data based on the BCS framework to support investment decisions

INSURERS, LENDERS, & INVESTORS

A standardized framework for insurers, lenders, and investors to facilitate physical cyber risk assessments and set differentiated fee structures and investment grade ratings

Real estate platforms recognized at each certification level in terms of ability to safely offer an array of smart technology management services

Benefits of Protecting Building Management Systems

As smart technology services expand, new safety and protection services will be required.

Protecting building management systems will reduce risks to:

- Life, Safety, Health – Protection of Employees & Visitors
- Bad Actions or Errors from Employees
- Outside Takeover of Operational Systems
- Business Interruption/Decline
- Brand Value

How many IoT devices are connecting to the internet every second worldwide?

A. About 50 devices?
B. About 75 devices?
C. About 100 devices?
D. About 125 devices?
E. About 150 devices?

11 million devices / day

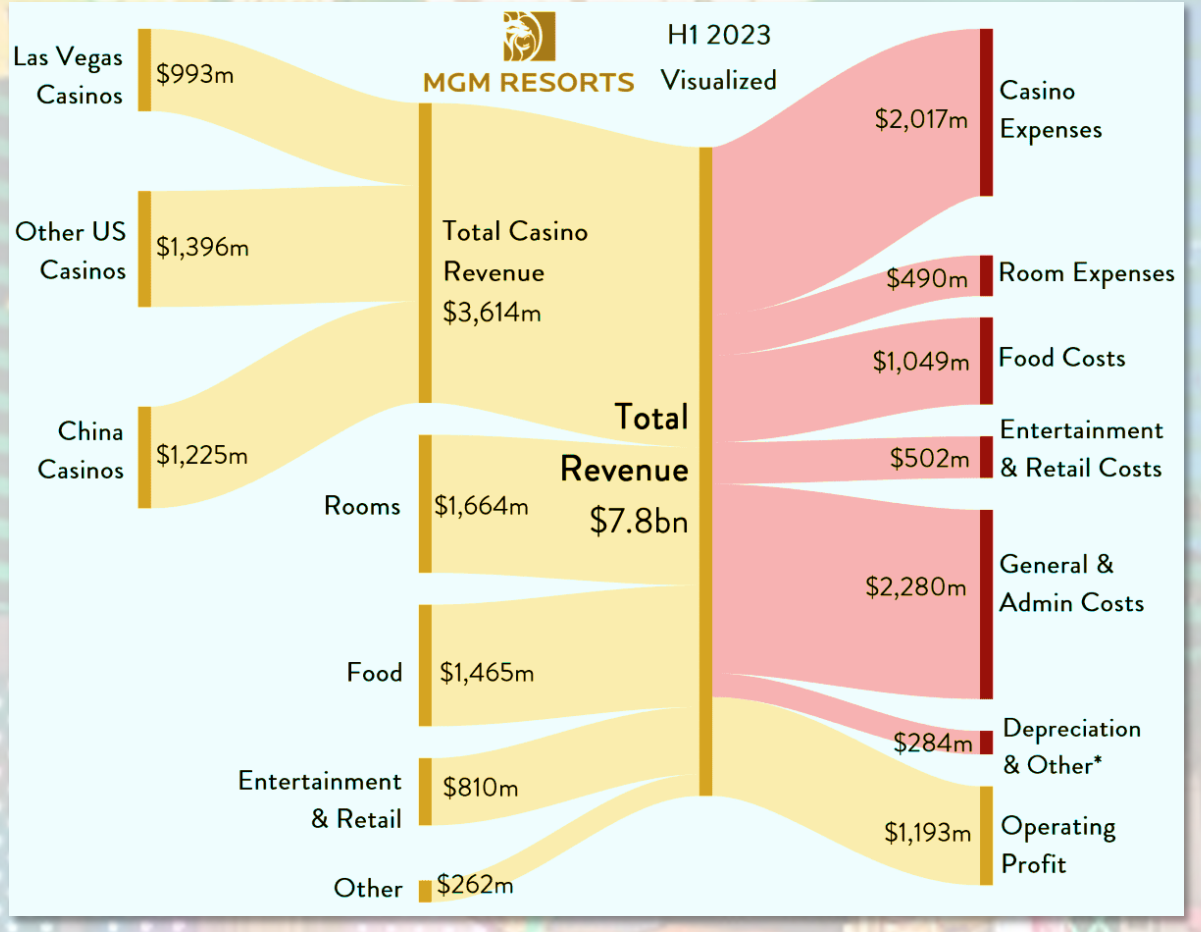
CASE STUDY-1: Sep 11, 2023, ransomware attack on MGM Resorts resulted in 10 days of system downtime & loss of ~$80,000,000 by threat actor dubbed "Scattered Spider" and alleges to have ties with the infamous ALPHV/BlackCat ransomware gang.

How much is MGM resorts losing per day due to the hack?

A. $ 1.1 million?
B. $ 2.4 million?
C. $ 5.5 million?
D. $ 8.4 million?

Systems impacted:

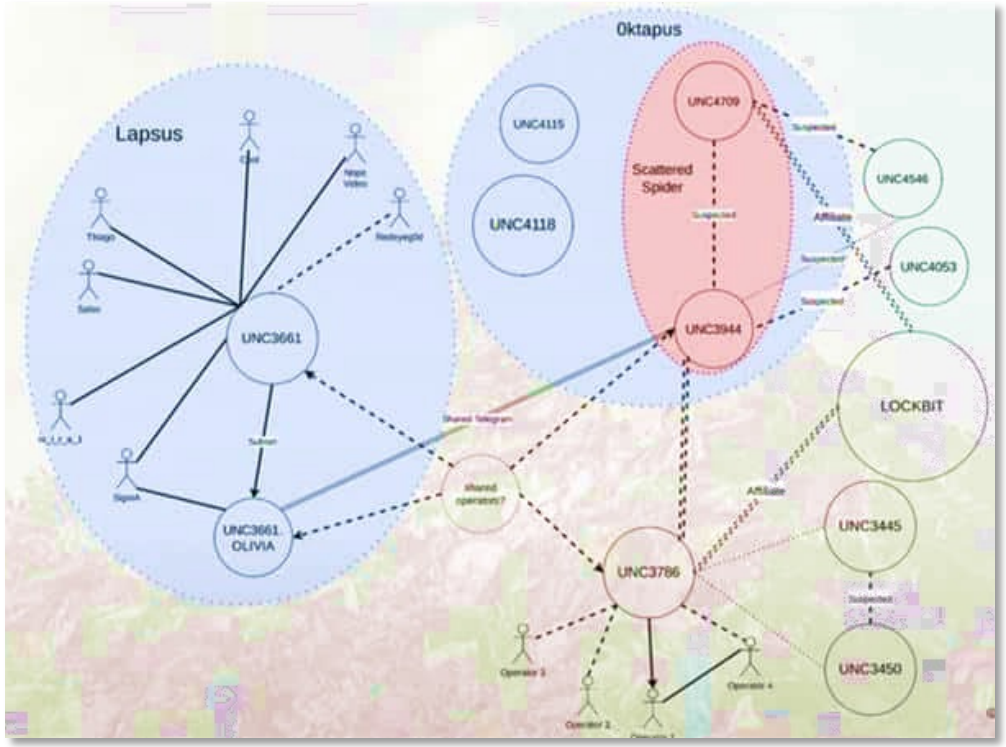
- ✓ Casinos
- ✓ Phone lines
- ✓ TV service in hotel rooms
- ✓ Reservation systems
- ✓ Payroll systems
- ✓ Access to key cards for hotel guests



https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.chartr.co%2Fnewsletters%2F2023-09-20&psig=AOvVaw2hWeDjmOk-UqMMsKed3XE_&ust=1701201297538000&source=images&cd=vfe&opi=89978449&ved=0CBAQjRxqFwoTCJCDjOz65IIDFQAAAAAdAAAAABAD

“Scattered Spider” @ MGM Grand, Cont.

- **Sept 2023 - The Com’s "Star Fraud,“hacked MGM, Caesars, Clorox and other major corporations:**
  - The MGM breach disrupted operations at casinos/hotels with hotel room digital keys, elevators, slot machines not working; estimated costs of $80 million in damages, per an MGM October Regulatory filing.
  - Caesars paid around $15 million in ransom to regain access to its systems from the hackers.
- **Scattered Spider relied heavily on social engineering to break into company networks:**
  - Manipulated victims into performing actions by impersonating people the victim has a relationship with
  - Started as phishing asking employees to reset their passwords or share their login credentials
  - A SIM swapping attack allowed access someone's multi-factor authentication code.
  - Convinced the company's IT help desk to reset the victim employee's password
  - Used seemingly normal remote work tools to exfiltrate data without raising suspicions.



- Use of fear-mongering tactics - targeting individuals through phone calls/texts with personal information (home addresses and family names) to coerce victims into sharing credentials for corporate access.
- Scattered Spider-linked hackers threatening to kill employees unless they provided passwords.

CASE STUDY-2: Former Service Provider Employee Destroys Equipment

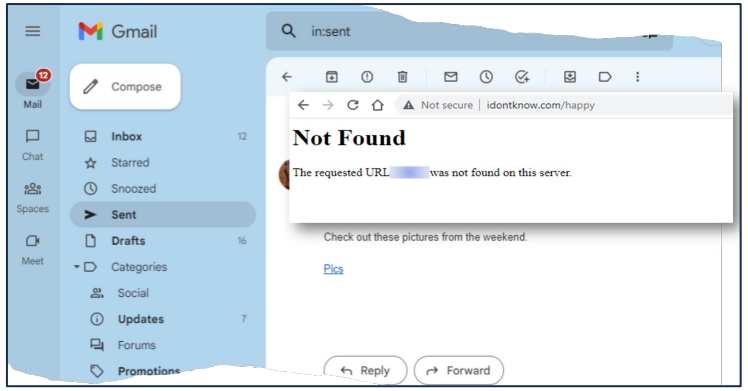
- ✓ One in three ex-employees are left with access to systems or data after leaving a company. (7)
- ✓ 75% of insider threat cases involved a disgruntled ex-employee who left with company data, destroyed company data, or accessed company networks after their departure. (8)
- ✓ In a recent study, Beyond Identity gathered responses from former employees found 83% of employees admitted to maintaining continued access to accounts from a previous employer. (9)

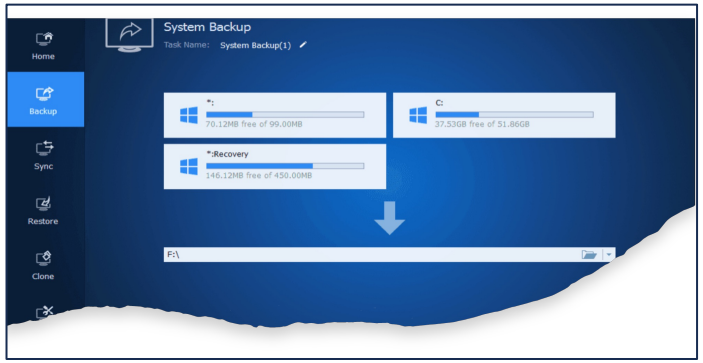
- ✓ Typically service providers are not required to notify asset owner when one of their employee no longer needs access to the system they service.
- ✓ Over 75% of service provider use a single account to access the system they support.
- ✓ The majority of system service providers control remote access to system they support to both their employees and the asset owners.
- ✓ Most systems do not monitor access.

(7) https://www.isdecisions.com/blog/it-security/a-third-of-ex-employees-accessing-company-data/
(8) https://www.informationweek.com/cyber-resilience/75-of-insider-cyber-attacks-are-the-work-of-disgruntled-ex-employees-report#close-modal
(9) https://www.helpnetsecurity.com/2022/02/21/employees-maintaining-accounts-access/

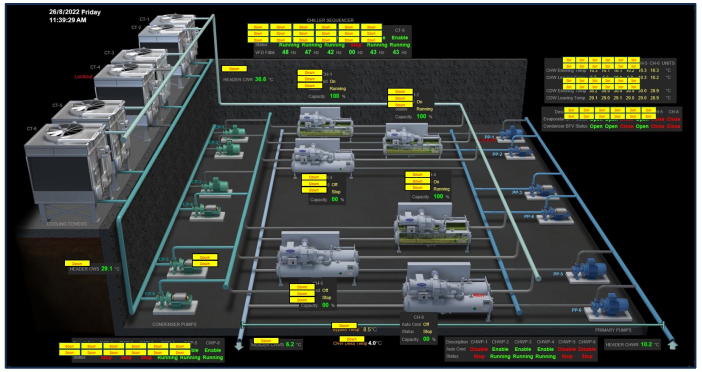
CASE STUDY-3: 92 Days to Recover

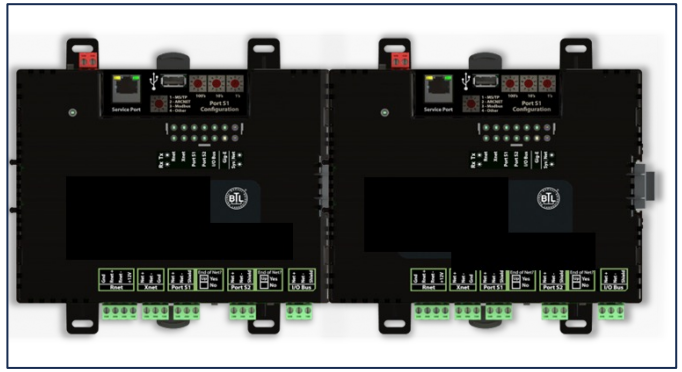
DAY 1

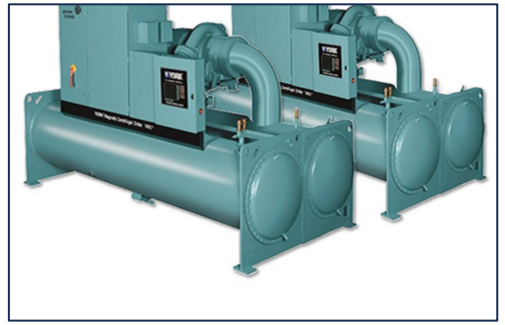




DAY 2

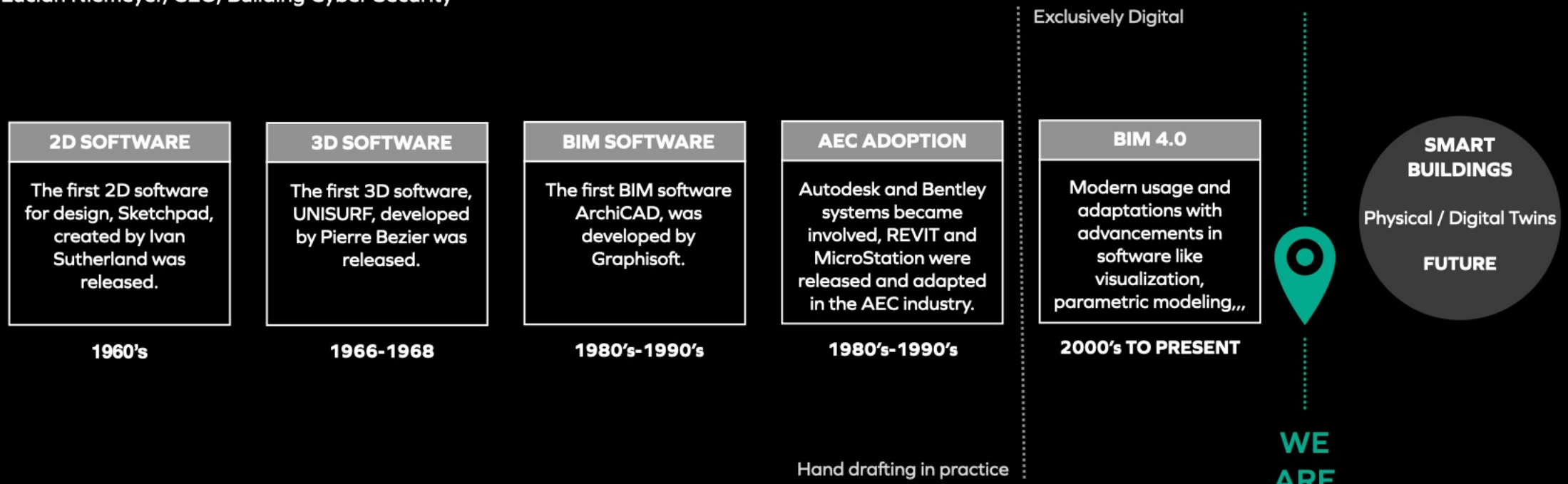






"There is the immediate need for Digital Twin templates/formats that the AEC industry will meet at minimal cost that is the next logical step in BIM."

Lucian Niemeyer, CEO, Building Cyber Security



This is movement level-change, expect massive growth in market and sophistication.

	SUSTAINABILITY	CYBER-PHYSICAL
LEADER	Architect of Record (AOR) & Sustainability Consultant	Technologist of Record (TOR)
THREATS	Climate Change, Resources	Bad actors, Security, Unawareness
BENEFITS	Healthier and Sustained EXP	Total (early) Integration
GOVERNANCE	USGBC, LEED,,, WELL, ...	Opportunity

11 BILLION SF

USGBC surpassed 100,000 LEED-certified projects globally in 2022, totaling more than 11 billion certified gross square feet. Since it was first established in 2000, LEED's metrics-based system has set the standard for healthy, resilient, green buildings.

www.geniant.com

We are a next-generation experience consulting company.

"Our mission is to ensure the integrity of a company's brand experience across physical space, human interactions, and digital-enabled moments.

space

People need great spaces in which to live, work, shop and play. With our unique, holistic research methods, our architects and interior designers create effective, performant spaces that improve employee retention, productivity, and customer engagement.

- Employee Experience for Hybrid Work
- Space Optimization Analysis
- Consumer Retail Strategy
- Architecture + Interior Design
- Retail Environments
- Digital / Physical Channel Integration
- Workspaces for Teams
- Rapid Concept Development
- Metaverse & VR Design

people

Every interaction, process and organization should be thoughtfully researched and designed. From services and operations to employee experience and culture, we optimize your workforce and help design and manage organizational change.

- Workplace Culture Assessment
- Workplace Programming & Strategy
- Innovation Consulting
- Service Design
- Employee Experience Strategy
- Customer Experience Journey
- Organizational Design
- Employee Productivity
- Digital & Physical Accessibility
- Change Management
- Technical Organization Readiness Analysis

digital

Digital should be seamless across every touchpoint. With experience capabilities spanning strategy, design, and development, our research-driven methodology helps accelerate innovation and transformation at scale.

- Digital Transformation
- Digital Product Strategy
- Experience Design & Innovation Programs
- Behavioral Analytics
- Omnichannel Solutions
- Web & Mobile Development
- Digital Workplace Solutions
- Software Development
- ML & AI Solutions
- Enterprise Architecture
- Design Systems

www.geniant.com

Thank you!

KMC Consulting™
Trusted Advisors

Please direct questions or inquiries to:

- Ari Reubin
- SVP | KMC Consulting (a division of KMC Controls)
- C: 214.395.8880
- Schedule a meeting with Ari
- LinkedIN
- https://www.kmccontrols.com/consulting

- **Core Mission:** Serve as trusted advisor to decision makers in commercial, institutional, and government entities around the globe (https://www.kmccontrols.com/consulting)
- **Core Clients:** Owners & Operators of and Solution Providers to Commercial & Institutional entities
- **Core Specializations:**
  - ✓ Decreasing real-time and predicted risk in buildings and other built environments
  - ✓ Improving safety and the sense of well-being
  - ✓ Decreasing cyber-physical vulnerabilities