

REAL ESTATE SUPPLY CHAIN CYBERSECURITY

EXPLORATORY ANALYSIS OF THE THREATS AFFECTING THE
SUPPLY CHAIN OF REAL ESTATE AND CONSTRUCTION SECTORS

**IN DEPTH OVERVIEW OF THE
VULNERABILITIES POSED BY
DIGITAL TECHNOLOGY
THREATS TO THE SUPPLY
CHAIN AND OPERATIONS OF
REAL ESTATE AND
CONSTRUCTION AND THEIR
IMPACT ON THE ECONOMY
AND OTHER SECTORS**



The background of the image is a light gray surface populated with numerous 3D house models. Most of these models are a uniform light gray color. One model, located slightly to the right of the center, stands out with a bright red roof. The houses are scattered across the frame, some appearing closer and larger, while others are further away and smaller, creating a sense of depth. The lighting is soft and even, casting gentle shadows from the houses onto the surface. The overall aesthetic is clean, modern, and minimalist.

THE STATE OF REAL ESTATE CYBERSECURITY

CYBERCRIME IN REAL ESTATE

Phishing/Scams: Perpetrators will spoof accounts and often impersonate someone from within the company in attempts to obtain more access or information

Wire Fraud: Criminals will attempt convincing the business into sending a wire to wrong accounts by posing as escrow agents, attorneys, and even buyers/clients (IC3, 2021)

Ransomware: RE companies are seeing a rise in attacks of information availability due to the increased reliance on business and information systems for their operations (IC3, 2021)

IoT Vulnerabilities: From printers to other devices connected to the internet are opening ways for hackers to intercept networks due to poor security standards (i.e.: printers without WPA2 protocol)

Trojans: Oftentimes, RE agents might not be properly trained to distinguish legitimate websites, emails, and have poor internet hygiene leading to banking trojans and more

Data Breaches: As in many other industries, data breaches are a leading cause for slowdowns, reputation damage, and financial loss

WHAT MAKES REAL ESTATE AN ATTRACTIVE TARGET?



The type of data involved in the business which can include financing data, lease and rental application information, credit reports and PCI related data, bank statements, and all sorts of PII (KPMG, 2018)



A slew of vulnerabilities ranging from technical (IoT, lack of protocols, outdated systems) to the human element (email communications, lack of training, poor internet habits) (IC3, 2021)



Real estate is a profitable business often involving high value transactions, lucrative deals, wide range of assets, and large amounts of financial information (Deloitte, 2015)



WHERE ARE THE RISKS?

- **Leadership:** Executives and senior management personnel lack ability to establish proper cybersecurity roadmaps (KPMG, 2018)
- **Social Engineering:** Call center teams, receptionists, and real estate agents all fall victim to social engineering tactics, often by perpetrators faking to be someone from senior management, attorneys and escrow agents, and even clients (IC3, 2021)
- **Lack of Training:** Absence of cyber awareness policies at all levels, from senior management to RE agents to third party contractors (Deloitte, 2015)
- **Internal Threats:** Insider threats coming from current and former employees, access issues, no culture of security,
- **Third-Party Vendors (Perimeter Protection):** Insufficient security programs and standards by external contractors and third-party suppliers, contractors, and subcontractors pose threats to even the most protected companies (KPMG, 2018)
- **Underdeveloped cybersecurity plans/response:** Need for development of cyber breach response plans and culture/mentality of “not if, but when” (EY, 2018)

Which of the following risks are you most concerned about?

Cybersecurity risk

38%

Regulatory risk

34%

Geopolitical risk

26%

Third-party risk

24%

Emerging technology risk
Strategic risk

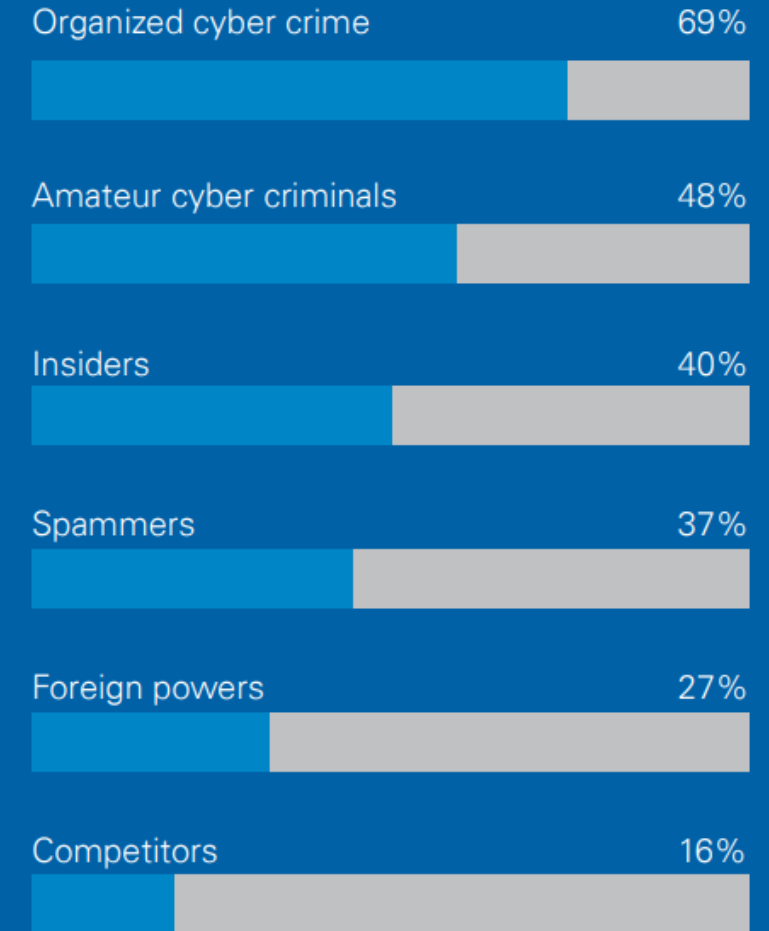
23%

Source: U.S. CEO Outlook Survey (KPMG, 2016)

WHO ARE THE BIGGEST THREATS?

- **Common attacks:** These types of attacks are often carried out by amateur cybercriminals and include email phishing and cellphone smishing campaigns, low-quality social engineering attempts, and easily detectable schemes or known threats/vulnerabilities (EY, 2018)
- **Sophisticated attacks:** In contrast to the common types of threats, refined attacks carry a heavier toll for RE agencies and companies, posing high risks and are often carried out by organized crime networks and nation states especially during Covid-19 and the movement towards digital transformation
- **Rising threats:** These attack vectors are due to new technologies and the increasing reliance on IoT and IIoT from coffee machines to smart buildings (Gartner, 2021)

Which types of threat give you most cause for concern in terms of a cyber attack?



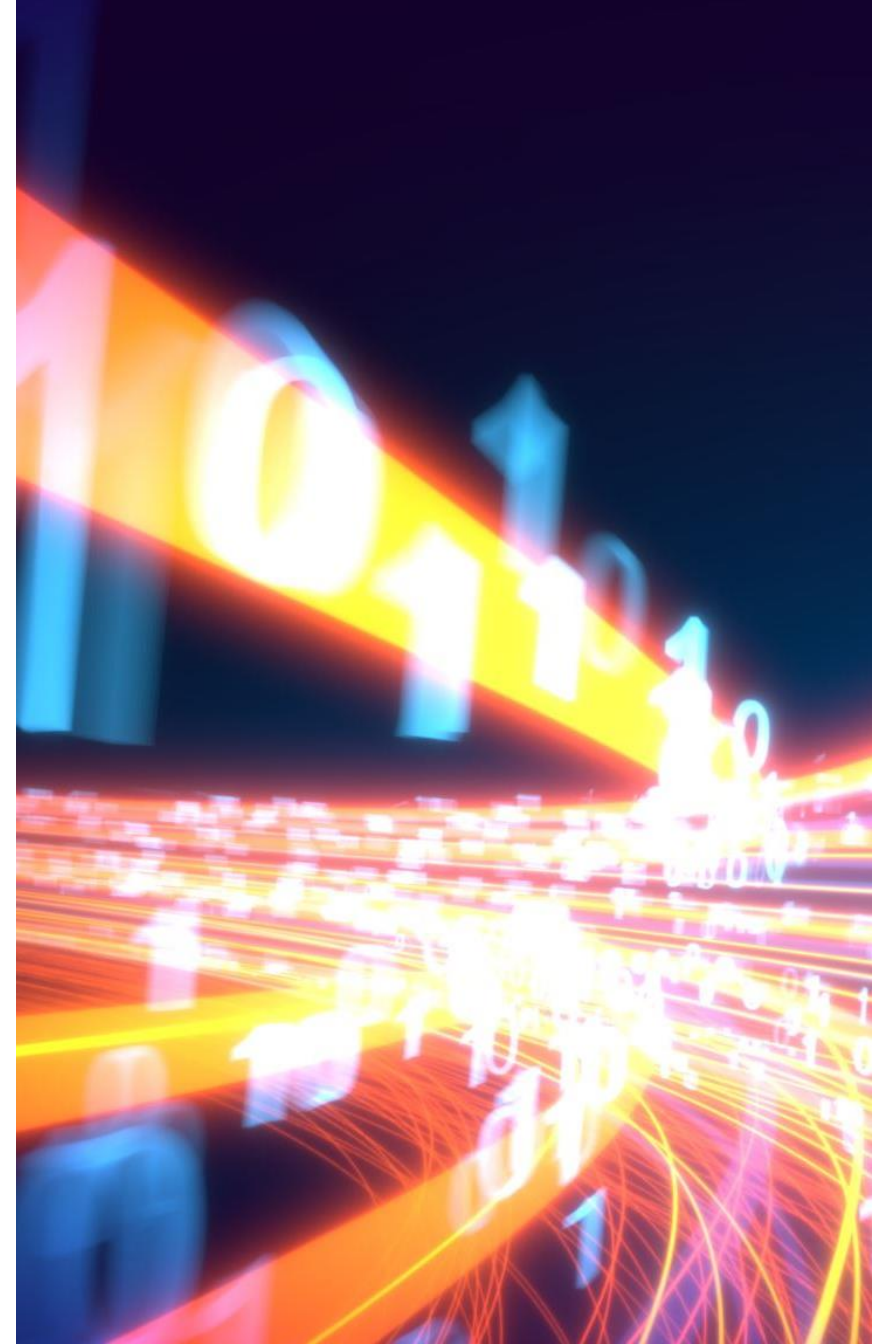
⁵ The Creative CIO: Harvey Nash/KPMG CIO Survey 2016 (Harvey Nash/KPMG, 2016)
data is global and cross-industry



INDUSTRIAL INTERNET OF THINGS AND THE DIGITAL TRANSFORMATION

THE AGE OF DIGITAL TRANSFORMATION

- As the pandemic developed more and more vulnerabilities have deepened as hybrid workforces, remote work and the sudden need to create a social distance work environment have accelerated the deployment of digital solutions
- The rise and growth of new cloud technologies, client portals and mobile and web-based apps have opened doors for emerging threats to all sectors (PWC, 2022)
- Companies have accelerated the digitization of their customer and supply-chain interactions and of their internal operations by three to four years (McKinsey, 2020)



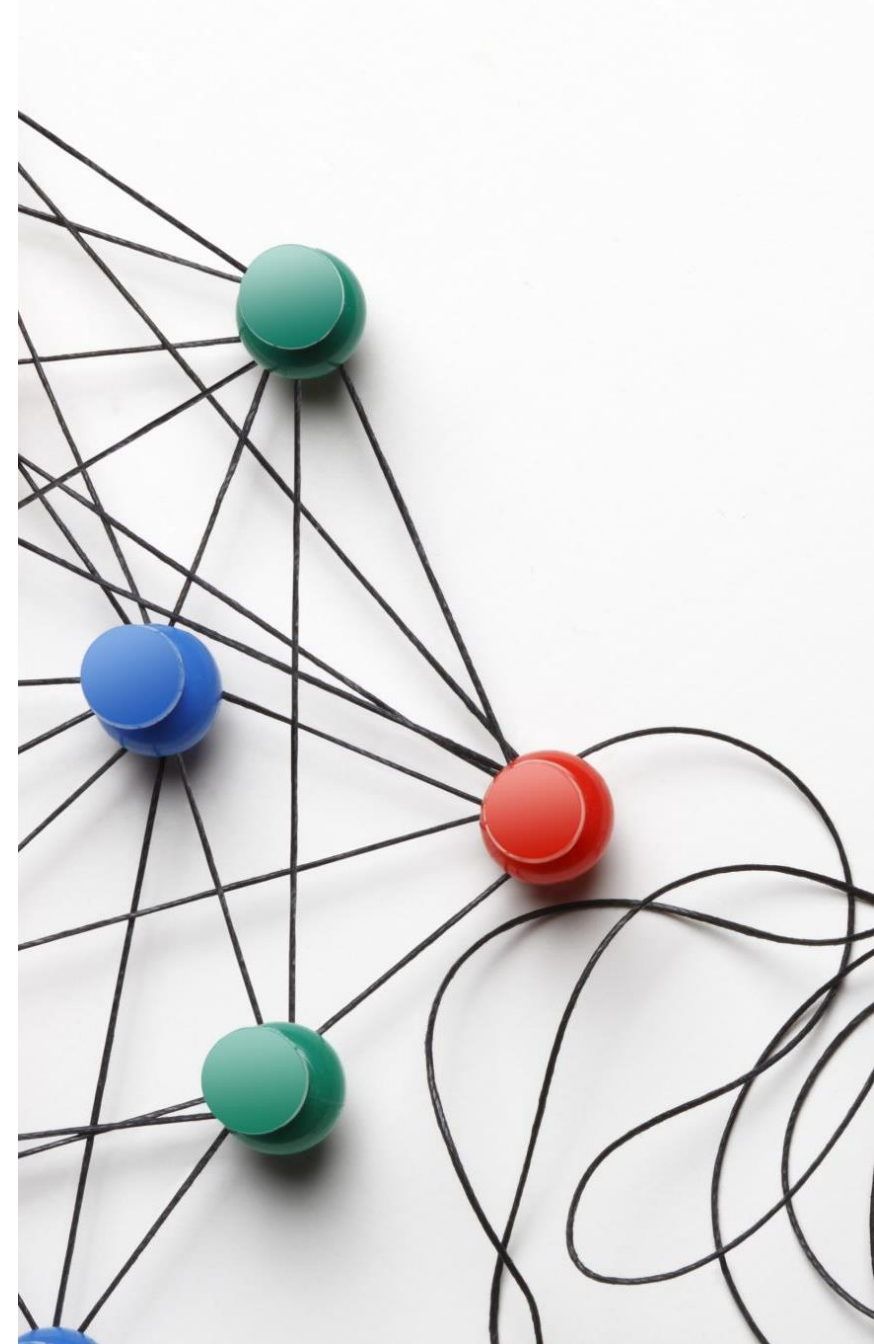
AUTOMATION AND THE CYBER PHYSICAL DOMAIN

- **Cyber physical systems (CPS)**, smart buildings, interconnected ecosystems, and the spread of internet of things into industrial facilities and commercial real estate are giving way for emerging threats and new vectors of attack (Gartner, 2021)
- **Automation and robotization** of production lines, building facilities, industrial networks, and the convergence of cyber and physical domains are broadening the surface for attacks and increasing the risk of vulnerable environments unknown for leaders
- **Digital transformation** from a business perspective has acted as a catalyst for increased use and reliance on cutting-edge technology that is poorly understood by business leaders
- **Operational technology** vulnerabilities are a rising due to the complex nature of the mesh of networks created by the increased use of CPS (Gartner, 2021)
















































INDUSTRIAL INTERNET OF THINGS AND CPS HACKS

- **Emerging smart building technologies** including sensor enabled heating and cooling systems, alarm systems, door access and security systems
- 2016 attack on Finnish **computerized heating distribution centers disabled heat to apartment buildings** (BDO, 2017)
- Springhill Medical Center is being sued for what could be **the first death directly attributable to ransomware**, when clinical devices became unusable (Gartner, 2021)
- Colonial Pipeline **stopped all its fuel processing for days** when it fell victim to a ransomware attack
- An attacker managed to **physically move gauges** in Oldsmar, Florida



OVERVIEW OF SYSTEMS AND INFRASTRUCTURE

Systems involved	Owner/tenant	Owner/tenant	Owner	Owner/tenant	Owner/tenant	Owner
Entry points by property type	Mobile/web applications	Online payments/point of sale (POS)	Industrial control systems/HVAC/BMS	Employee devices	Webserver/network/cloud	Open Wi-Fi access
Hotel						
Retail						
Health care						
Multifamily						
Data center						
Office						
Industrial						
 High  Medium  Low						

Source: Deloitte Center for Financial Services Analysis

A photograph of an industrial facility, likely a refinery or chemical plant, at sunset. In the foreground, large, cylindrical storage tanks are visible, supported by metal structures. The tanks are illuminated by the warm, orange light of the setting sun. In the background, the industrial complex is lit up with various lights, and a tall distillation column is visible. The sky is a mix of orange, yellow, and blue, with some clouds. The overall scene conveys a sense of industrial activity and infrastructure.

REAL ESTATE SUPPLY CHAIN AND CRITICAL INFRASTRUCTURE

CYBERCRIME AND THE SUPPLY CHAIN CRISIS

- **Covid-19 acted as a catalyst** for many manufacturing and logistic companies to increase reliance on digital and automation technologies and business systems
- Cyberattacks on manufacturing companies spiked by over 300% during 2021 according to the Global Threat Intelligence Report (PWC, 2022)
- Cyber supply chain risks is **more than an IT problem** (people, process, knowledge, infrastructure)
- Increased phishing and ransomware attacks affecting manufactures and suppliers

Manufacturers making progress in aligning cyber with overall business strategy

Increased number of business decisions made that involved input from the enterprise security management team



Increased percentage of security requests that are being fulfilled by customers



Increased number of mergers and acquisitions that involve cybersecurity considerations



Increased number of cybersecurity vendors that undergo regular cyber risk assessments



Increased number of business units that assign risk responsibility for addressing cyber as it relates to the impact on the organization



Increased percentage of overall risk remediation being completed by proposed deadlines from security team



Increased alignment of cyber strategy to business strategy



Significant progress

Moderate progress

Source: 2022 PwC Digital Trust Insights survey, 202

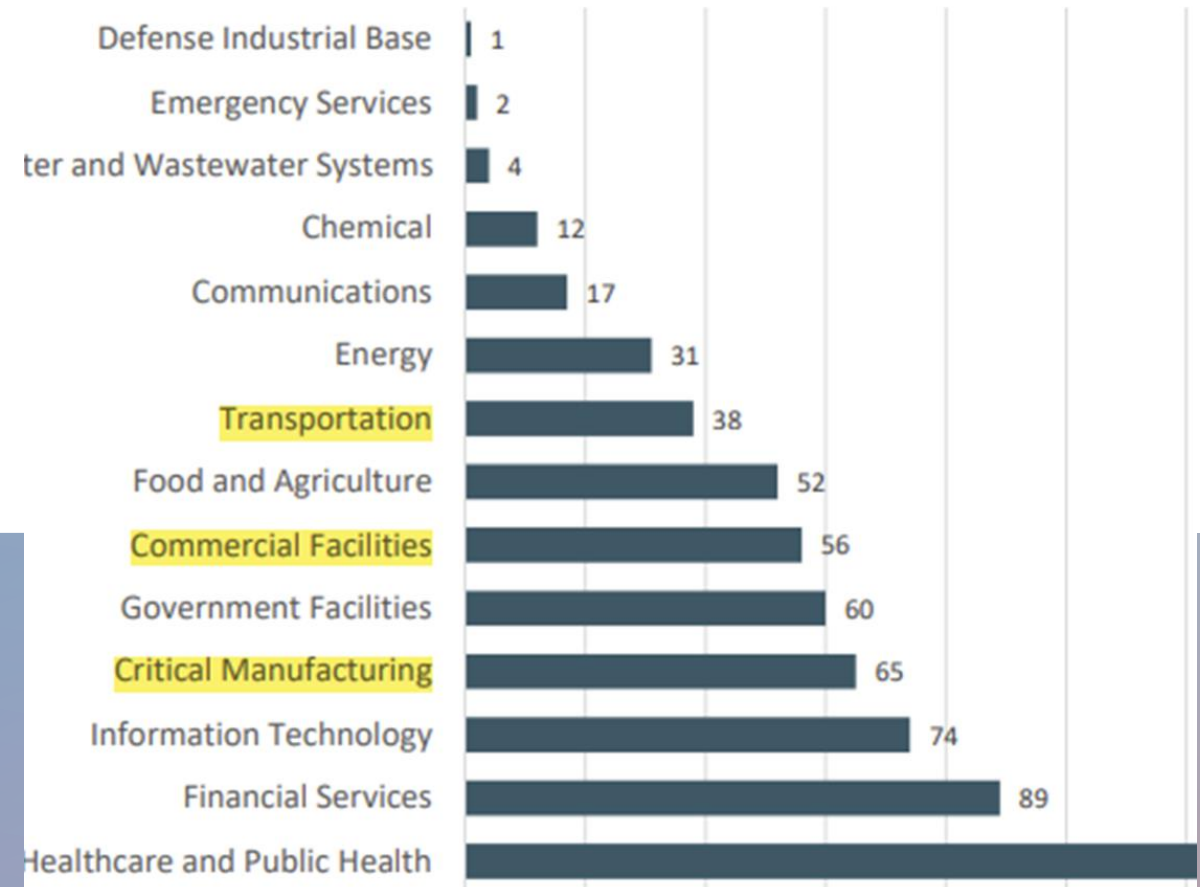
REAL ESTATE CRITICAL INFRASTRUCTURE

- Difficulties associated with **securing complex manufacturing processes and operational technology** from any sector that uses industrial control systems (BDO, 2017)
- Many of the 16 CI sectors are **within the scope of real estate and construction industry**, from logistic systems, transport networks, government and commercial facilities, and defense industry bases (BDO, 2017)
- Construction companies contracting with the government must also consider their **subcontractor's cybersecurity standards**: Any weak cyber link can create a vulnerability
- **California added real estate to its list of critical infrastructure** including industrial, commercial, residential and sheltering facilities and services (California Essential CI, 2020)



OVERVIEW OF AFFECTED INDUSTRIAL SECTORS

Infrastructure Sectors Victimized by Ransomware



COSTS, IMPACTS, AND THE ECONOMY



WHAT ARE THE IMPLICATIONS?

Loss of data - either company financial data, customer, or project information

Compromised employee information and payroll systems

System and/or server shutdown

Stolen intellectual property

Lawsuits stemming from the failure to protect certain types of data

Fees to get systems back online

Ransom paid to hacker groups

Regulatory fees/penalties

Reputational damage

Involuntary downtime

THE COSTS OF CYBERCRIME

- Smaller companies run a high risk of going out of business
- Slowdowns in development, causing delays worth thousands and potentially millions of dollars
- All actors involved in the supply chain are affected (in real estate usually there are many parties with an investment)



IMPACTS OF DATA BREACHES



July 19, 2017



Dear Sample A Sample,

Notice of Data Breach

Keller Williams Realty, Inc. recently experienced a potential security incident involving the personal information of some of its current and former associates. We are providing this notice as a precaution to inform potentially affected individuals of the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We recently learned that an unauthorized third party was able to gain access to portions of the Keller Williams network and, while on the network, may have been able to access certain associate files stored in our systems.

What Information Was Involved

We believe that certain associate and information, including first and last name, addresses, Social Security number, and in some cases, Keller Williams usernames and passwords, were contained in these files and could be affected as a result of this incident. Please note that at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

Keller Williams takes the privacy and protection of personal information very seriously, and deeply regrets that this incident occurred. Upon learning of this situation, we took immediate action to identify, block and prevent future unauthorized access, and initiated an investigation with the assistance of external forensic experts. In addition, we have contacted law enforcement and will continue to cooperate in their investigation of this incident.

To help protect your identity, we are offering a complimentary membership in Experian IdentityWorksSM. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks at no cost to you. To enroll in these services, visit <https://www.experianidworks.com/creditone> by **October 31, 2017**, and use the following activation code: **ABCDEF GHI**.

0 03458



C0235-103



<<MemberFirstName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Esta carta contiene informacion importante. Para la version en espanol porfavor llame al 1-877-451-9366.

NOTICE OF DATA BREACH

Dear <<MemberFirstName>> <<MemberLastName>>,

What happened?

On March 2, 2016, certain personal information was disclosed in an email to an unauthorized recipient. We immediately began investigating and engaged third party experts to assist us with this response. Subsequently, we determined that your personally identifiable information was disclosed in this email to an unauthorized recipient.

Since discovering the unauthorized disclosure, we have notified federal, state and local law enforcement of this incident. We are consulting with legal, law enforcement, information technology and security experts and will follow their recommendations to protect the affected persons and to ensure that this type of disclosure will not again occur.

What information was involved?

As a result of this incident, other persons or individuals may have obtained some of your personal identifying information which included your full name, Social Security number, name of each state in which wages or taxes are reported for the affected residents, and federal, state, local and Medicare earnings and tax withholding data. This did not include any information on spouses, dependents, bank account or direct deposit information. It did not include your address or date of birth. We are informing you of this incident and have set forth the below measures you may take in an effort to help protect your personal information.

What we are doing.

Turner Construction Company has provided the data that was disclosed to the Internal Revenue Service. The Internal Revenue Service has taken steps to monitor your tax account for suspicious activity.

Turner Construction Company has secured the services of Kroll to provide identity monitoring to you and your spouse or partner at no cost to you for ten years. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Theft Insurance, Identity Consultation, and Identity Restoration.

Visit kroll.idMonitoringService.com to enroll and take advantage of your identity monitoring services.

Membership Number for <<MemberFirstName>> <<MemberLastName>>: <<Member ID>>

If you have a spouse or partner that would like to enroll in identity monitoring services, please have your spouse or partner use the membership number below.

Membership Number for your spouse or partner: <<ClientDef1(SpousePartnerNumber)>>

To receive credit services by mail instead of online, please call 1-877-451-9366. Additional information describing your services is included with this letter. We urge you to review the description and to consider enrolling in this product. **You must complete the enrollment process by no later than June 1, 2016.**

For more information please contact Kroll's call center.

In order to more efficiently answer any questions you may have related to this incident, Turner has established a call center service so that you can speak with a live operator. If you have questions, please call 1-877-451-9366, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

03091-0316

OVERVIEW OF FINANCIAL IMPACT BY INDUSTRY

2021 Crime Types continued

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$2,395,953,296	Lottery/Sweepstakes/Inheritance	\$71,289,089
Investment	\$1,455,943,193	Extortion	\$60,577,741
Confidence Fraud/Romance	\$956,039,740	Ransomware	*\$49,207,908
Personal Data Breach	\$517,021,289	Employment	\$47,231,023
Real Estate/Rental	\$350,328,166	Phishing/Vishing/Smishing/Pharming	\$44,213,707
Tech Support	\$347,657,432	Overpayment	\$33,407,671
Non-Payment/Non-Delivery	\$337,493,071	Computer Intrusion	\$19,603,037
Identity Theft	\$278,267,918	IPR/Copyright/Counterfeit	\$16,365,011
Credit Card Fraud	\$172,998,385	Health Care Related	\$7,042,942
Corporate Data Breach	\$151,568,225	Malware/Scareware/Virus	\$5,596,889
Government Impersonation	\$142,643,253	Terrorism/Threats of Violence	\$4,390,720
Advanced Fee	\$98,694,137	Gambling	\$1,940,237
Civil Matter	\$85,049,939	Re-shipping	\$631,466
Spoofing	\$82,169,806	Denial of Service/TDoS	\$217,981
Other	\$75,837,524	Crimes Against Children	\$198,950
Descriptors**			
Social Media	\$235,279,057	Virtual Currency	\$1,602,647,341

A long, straight road stretches over a body of water towards distant mountains under a cloudy sky. The road is flanked by dark railings, and the water reflects the sky. The mountains in the distance are hazy and blue. The sky is filled with soft, white clouds. The overall mood is serene and expansive.

BEST PRACTICES

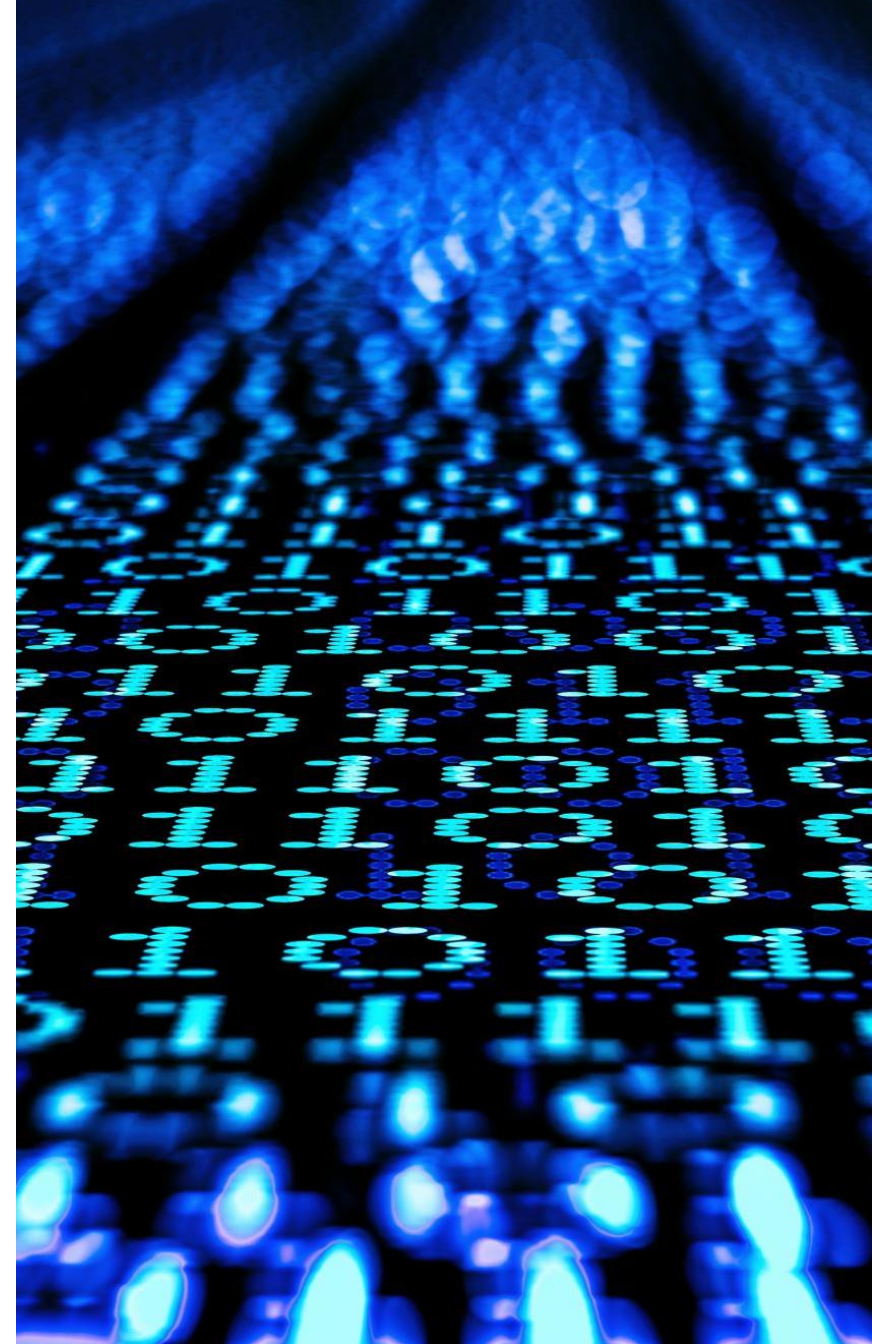
REAL ESTATE CYBERSECURITY

- **Ensuring proper internet habits and information security hygiene** including email and password verification, validation, management, and sharing. (Training against phishing tactics, sender confirmation, user credential management)
- **Development and establishment of a culture based around security** and protection of data and systems, including two-factor authentication, email/password encryption, Wi-Fi security.
- **From a technical perspective**, usage of antivirus and firewall management, database backups, network security, active response plans.
- **Close collaboration with legal department** for proper written disclosure notices, ensuring up to date knowledge of laws and policies surrounding cybersecurity and real estate
- **Policy management** including document retention/destruction, data security standards, breach response notice
- Consider having **cyber liability insurance** coverage



SUPPLY CHAIN CYBERSECURITY

- A major point for security of supply chain and manufacturing systems rely deeply on having a **culture of security** and accepting that cybersecurity problems exist and create a risk to the bottom line (“it’s just a matter of time” mentality)
- **Proper update and patchwork** of firmware, software, and hardware around all automation technology and systems (this includes anything from printers to assembly machines to HVAC systems)
- **CPS security** is key to remediate the growing gaps between the physical and digital interconnected systems (NIST CSCBP)
- **Third party services** such as software engineering all the way to janitorial services, suppliers, hardware providers, and anyone or anything that may impact physical security of systems (perimeter protection)
- **Onsite physical security**, many manufactures and companies from all industries have solid public interface security, but what about someone with a laptop on premise, a contractor with enough access, or an unlocked door into an IT room or important office



ENDNOTES

- **EY**, Cybersecurity regained: preparing to face cyber attacks 20th Global Information Security Survey 2017-18, 2018
- **KPMG**, Securing Real Estate Assets in a Digital World: How internal audit can focus your organization's cybersecurity, 2018
- **NAR**, CYBERSECURITY CHECKLIST: Best Practices for Real Estate Professionals, 2020
- **Deloitte**, Evolving cyber risk in commercial real estate. What you don't know can hurt you, 2015
- **Gartner**, 3 Initial Steps to Address Unsecure Cyber-Physical Systems, 2021
- **BDO**, Real Estate and Construction Monitor, 2017
- **RCG**, Housing is Critical Infrastructure: Social and Economic Benefits of Building More Housing, 2021
- **Executive Order N-33-20**, Governor Newsom, 2020
- **McKinsey & Company**, How COVID-19 has pushed companies over the technology tipping point and transformed business forever, 2020
- **FBI**, Internet Crime Report, 2021
- **NIST**, Best Practices in Cyber Supply Chain Risk Management
- **Propmodo**, A New, Turbulent Era for Real Estate Supply Chains, 2022
- **PWC**, Manufacturers ramp up cyber defenses as supply-chain bottlenecks and vulnerabilities deepen, 2022
- **NIST**, C-SCRM Fact Sheet, 2022