

PRESENTED BY



Rea & associates
a brighter way

ELEMENTS OF RISK IN CONSTRUCTION

9.17.20



HOST



Doug Houser, CPA, MBA, CEPA

Principal

Director of Construction & Real Estate Services

Doug.Houser@reacpa.com

(614) 314-5937



Scott Bechtel, CPA

Principal

Scott.Becht@reacpa.com

(614) 923-6547



CYBERRISK & COVID: WHERE WE ARE NOW

CONSTRUCTION & GENERAL CONTRACTING COMPANIES



Presenter

Shawn M Richardson, US Army (Ret)

- Principal, Cyber Services Segment
- Dublin, Wooster offices
- Director of Cyber Security Services
- Trusted Advisor, Speaker, Thought Leader

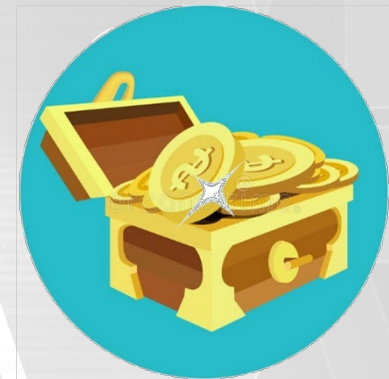


Agenda

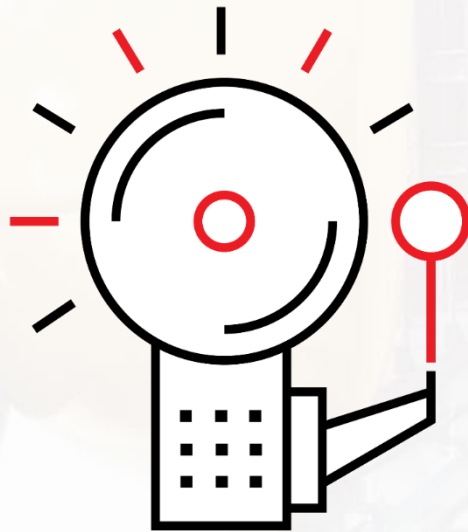
- 🌀 What are we doing for our clients now?
- 🌀 Cyber Risk & Breach's as a result of COVID
- 🌀 Re-Entry Recommendations
- 🌀 Our approach to Cyber Risk
- 🌀 Why Cyber Insurance?
- 🌀 Questions



- Company's scrambling – not prepared (BCP/DRP)
- Lack of expertise & oversight (MyISO/vCISO)
- No continuous monitoring – No one watching! (MDR/MSSP)
- Cyber Security has been overlooked – UNTIL NOW! (IGNITE/ISRA)



Three Primary Cyber Breaches (#1):



Not a breach, just an incident:

- The attack impacts availability of systems, but not Confidentiality or Integrity
- **MASSIVE IMPACT TO REVENUE DUE TO DOWNTIME AND INTERRUPTIONS**

Three Primary Cyber Breaches (#2):



The “Theft” breach:

- ⦿ Access is unauthorized
- ⦿ Compromised system includes access to assets
- ⦿ Fraud is executed through electronic transactions
- ⦿ Money/Assets/IP are stolen

Three Primary Cyber Breaches (#3):



The “Copy” breach:

- Our data is still there
- Our data is also stolen
- 6-9 months to discover
- \$1-3M in average costs, if it is found
- The single largest loss event (aggregate) world wide –and each year grows

Breach Example: Local Family Owned SMB

- 🌀 Ransomware (CryptoLocker) 4/6/20
- 🌀 Business did not have a Cyber Security Risk Framework or controls in place
- 🌀 Owner relied on local MSP to open network for employees to work from home through 3rd Party Vendor
- 🌀 Rea Cyber Incident Response Team (IRT) engaged
- 🌀 Recovery operations completed 4/16
- 🌀 Downtime – 10 days
- 🌀 Annual Sales – \$1.2-1.5m
- 🌀 Total operational business loss Est. \$35k
- 🌀 Total business without IRT - \$100k or more

Implementation & Monitoring

Testing & Updating

Reporting

Training

Controlling Access

Data Retention & Destruction

3rd Party Risk Management



Regardless of the current questions regarding cybersecurity expectations:

- 🌀 Multiple industry groups are forming to establish guidance
- 🌀 Launch & Implementation of CMMC
- 🌀 All states now have privacy laws
- 🌀 Several cyber bills are pending in State and Federal legislatures (Ohio Cybersecurity Safe Harbor Law – SB220)
- 🌀 Liability and fiduciary thresholds are being tested in current court cases
- 🌀 Cyber events/attacks are skyrocketing; up 400% since COVID

Regulation is coming for everyone.

Recommendations

What should businesses be doing now?

- 🌀 Conduct “Re-Entry Assessments” prior to re-entry to office
- 🌀 Training – prepare your employees and your clients for the inevitable
- 🌀 Set the expectation of Cybersecurity awareness, today. Bring in your professionals or trusted advisors (or hire one)
- 🌀 Utilize a viable and accepted framework to evaluate risk
- 🌀 Go on a “data-diet” today
 - 🌀 Assist your clients in doing the same
 - 🌀 Reduce the attack surface
 - 🌀 Treat data like cash
- 🌀 Do these five things now, right now:
 - 🌀 Backup and test your critical data, maintain proper patching, continuously inventory all of your assets, train your employees on threats, routinely audit access



Rea Cyber Approach

- 🌀 Unique hands-on approach to building a successful “Defense in Depth” cybersecurity roadmap directly aligned with clients’ business objectives
- 🌀 IGNITE Program – Cyber Security program w/ ISRA
- 🌀 DATA FIRST– Where’s your data? Is your data encrypted?
 - 🌀 (InfoGPS w/ DATAAnchor)
- 🌀 Framework focused – starts with a regulatory framework
 - 🌀 (K2 Compliance w/ all cross-walks)
- 🌀 Consistent Vulnerability Assessment – what's going on right now?
 - 🌀 Identify what’s hot sharp and dangerous to the business

Why Construction & GCs?

- Construction firms have access to a wealth of information that's desirable to hackers
 - Data including intellectual property
 - Proprietary assets
 - Building specifications & architectural drawings
 - Financial accounts (yours as well as your clients) all prime targets
- Examples construction & GC firms data can be breached:
 - Phishing, spear-phishing, and social engineering scams
 - Unlocked and misplaced/stolen employee laptops and mobile devices
 - Unauthorized access to company networks (both you and your clients)

What is Cyber Insurance

- 🌀 Our businesses are connected. Cyber insurance is a must for businesses, big or small, as cybercrime attacks grow in number and sophistication. Here are some facts that lead to more informed cyber insurance decisions.
 - 🌀 The number of data breaches continue to rise
 - 🌀 Small businesses are breached, too
 - 🌀 Breaches can happen to any business
 - 🌀 Breaches are getting more complex; complex breaches cost more
 - 🌀 Law requires immediate action; mandating prompt investigation, reporting, and customer notification
 - 🌀 Cyber coverage is affordable; is this all the coverage we need?

What is CMMC?

- 🌀 Cybersecurity Maturity Model Certification (CMMC)
 - 🌀 v1.02 & NIST 800-171 rev2 Compliance released 3/18/20
- 🌀 Think of CMMC as a procurement gate that a contractor must pass to even be eligible to bid on, win or participate on a contract - without a valid CMMC certification. Five levels
 - 🌀 CMMC Level 1: 17 Controls.
 - 🌀 CMMC Level 2: 72 Controls (includes Level 1 controls)
 - 🌀 CMMC Level 3: 130 Controls (includes Level 2 controls)
 - 🌀 CMMC Level 4: 156 Controls (includes Level 3 controls)
 - 🌀 CMMC Level 5: 171 Controls (includes Level 4 controls)
- 🌀 What's the deadline mean? (7/1/2020)
- 🌀 Framework crosswalk to other regulatory guidelines (NIST-CSF)

CMMC Crosswalk Example

Cybersecurity Maturity Model Certification (CMMC) v1.02 - People, Process & Technology (PPT) Breakdown

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (SA)	Situational Awareness (SA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.1.1001	AM.3.036	AU.2.041	AT.2.056	CM.2.061	IA.1.076	IR.2.092	MA.2.111	MP.3.122	PS.2.127	PE.1.131	RE.2.137	RM.2.141	CA.2.157	SA.3.169	SC.3.177	SI.1.210
AC.2.005	AM.4.226	AU.3.045	AT.2.057	CM.2.062	IA.1.077	IR.4.100	MA.2.112	MP.2.119	PS.2.128	PE.1.132	RE.2.138	RM.2.142	CA.4.163	SA.4.171	SC.2.178	SI.2.214
AC.2.006		AU.3.046	AT.3.058	CM.2.063	IA.2.078	IR.5.106	MA.2.113	MP.2.120		PE.1.133	RE.3.139	RM.3.144	CA.2.158	SA.4.173	SC.2.179	SI.4.221
AC.1.002		AU.2.042	AT.4.059	CM.2.064	IA.2.079	IR.2.093	MA.2.114	MP.2.121		PE.1.134	RE.5.140	RM.4.149	CA.2.159		SC.3.180	SI.1.211
AC.2.007		AU.2.043	AT.4.060	CM.2.065	IA.2.080	IR.2.094	MA.3.115	MP.3.123		PE.2.135		RM.4.150	CA.3.161		SC.3.181	SI.1.212
AC.2.008		AU.3.048		CM.2.066	IA.2.081	IR.2.095	MA.3.116	MP.1.118		PE.3.136		RM.4.151	CA.4.164		SC.3.182	SI.1.213
AC.2.009		AU.5.055		CM.3.067	IA.2.082	IR.3.098		MP.3.124				RM.2.143	CA.4.227		SC.3.183	SI.5.222
AC.2.010		AU.3.049		CM.3.068	IA.3.083	IR.4.101		MP.3.125				RM.3.146	CA.3.162		SC.3.184	SI.2.216
AC.2.011		AU.3.050		CM.3.069	IA.3.084	IR.5.102						RM.3.147			SC.3.185	SI.2.217
AC.3.012		AU.2.044		CM.4.073	IA.3.085	IR.5.108						RM.5.152			SC.3.186	SI.3.218
AC.3.017		AU.3.051		CM.5.074	IA.3.086	IR.2.097						RM.5.155			SC.3.187	SI.5.223
AC.3.018		AU.3.052				IR.3.099						RM.4.148			SC.3.188	SI.3.219
AC.3.019		AU.4.053				IR.5.110									SC.3.189	SI.3.220
AC.3.020		AU.4.054													SC.3.190	
AC.4.023															SC.3.191	
AC.5.024															SC.4.197	
AC.4.025															SC.5.198	
AC.2.013															SC.4.228	
AC.3.014															SC.5.230	
AC.2.015															SC.1.175	
AC.3.021															SC.1.176	
AC.4.032															SC.3.192	
AC.1.003															SC.3.193	
AC.1.004															SC.4.199	
AC.2.016															SC.4.202	
AC.3.022															SC.5.208	
															SC.4.229	

- Administrative (e.g., policies, standards & procedures)
- Assigned Tasks To Cybersecurity Personnel
- Technical Configurations(e.g., security settings)
- Assigned Tasks To IT Personnel
- Software Solution
- Assigned Tasks To Application/Asset/Process Owner
- Configuration of Software Solution
- Hardware Solution
- Configuration of Software or Hardware or Outsourced Solution
- Software or Hardware Solution



5 million apps, 6 billion connected people, 26 Billion devices, 3 million shortfall in InfoSec...

C. Roberts, 2018

QUESTIONS?



Shawn Richardson
Principal, Director of Cybersecurity Services
Wooster, OH
Shawn.Richardson@reacpa.com
(234)-249-3478



al word):
חינוכי
ormation:
-מידע; מא
to be used
licate or
a mic-
מכשיר
sounds
al ins-
על ידי
a own
...
insuperable adj (formal) = insurn
in-sup-port-able adj (formal)
insupportable rudeness. טה מנשוא
in-sur-ance n 1 nc, nu (an agreement
company or the State to provide) mon
ill health, death, loss of property etc
for a sum of money in case: take
£50 000 insurance. When her husband died
2 nc insurance (against something)
taken as protection against loss, failure
extra lock on the door as an insur
burglary. It is not apply for a course in
an insurance

INSURANCE RISKS



Presenter



Joe Urquhart, CPCU, CRIS, Vice President

- Commercial Insurance, Risk Management, and Bonding Consultant at Overmyer Hall Associates
- Specialties: Contractors, Real Estate Developers, and Manufacturers
- Builder's Exchange (BX) of Central Ohio President's Award Recipient
- Current or former member:
 - Safety Council of Greater Columbus (SCGC)
 - Associated Builders & Contractors (ABC)
 - American Subcontractors Association (ASA) of Ohio



Agenda

- Cyber Risk & Crime
- Cyber Liability
- Other Insurance Risks
- Update on COVID-19 Business Income Coverage & Liability
- Employment Practices Liability Risk
- Insurance Marketplace Review

Cyber Risk & Crime

Types of Cyber Risk & Crime: Defined

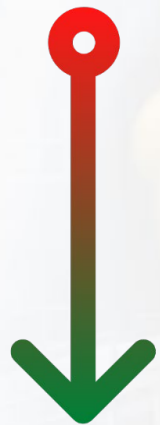
- Ransomware
- Social Engineering (wire transfer fraud)
 - Claims examples we're seeing locally

How to Protect Your Business: Risk Management

- Train, train, and more training
- Make informed decisions → work with professionals
 - Consult with your **CPA**
 - Consult with your **Bank**
 - Consult with your **IT firm**
 - Consult with your **Insurance advisor** & request a Cyber quote

Cyber Insurance

Levels of Cyber Insurance



No Coverage / Self-insure: Financial statement

Limited Coverage: Add on to General Liability

Crime Policy: Covers Social Engineering & Computer Fraud

Cyber Liability: 1st and 3rd party coverage + Crime

Cyber Liability: Insuring Agreements

- Liability
- Breach Response
- Cyber Crime
- Business Loss

Liability Insuring Agreements



PRIVACY AND SECURITY

- Coverage for claims arising from unauthorized access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorized users to gain system access, the participation in a DDoS attack, or the transmission of a computer virus.

MEDIA

- Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander, and violation of an individual's right of privacy or publicity in electronic and printed content.

REGULATORY

- Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.

Breach Response Insuring Agreements



PRIVACY BREACH NOTIFICATION

- Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call center services, notification, credit monitoring and the cost to purchase identity fraud insurance.

COMPUTER AND LEGAL EXPERTS

- Coverage for costs associated with analyzing, containing, or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed, or disclosed; and providing legal services to respond to such breaches.

BETTERMENT

- Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

CYBER EXTORTION

- Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.

DATA RESTORATION

- Coverage for costs to restore or recover electronic data, computer programs, or software lost from system damage due to computer virus, denial-of-service attack or unauthorized access.

PUBLIC RELATIONS

- Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.

Cyber Crime Insuring Agreements



COMPUTER FRAUD

- Coverage for loss of money, securities, or other property due to unauthorized system access.

FUNDS TRANSFER FRAUD

- Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution.

SOCIAL ENGINEERING FRAUD

- Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.

TELECOM FRAUD

- Coverage for amounts charged by a telephone service provider resulting from an unauthorized person accessing or using an insured's telephone system.

Business Loss Insuring Agreements



BUSINESS INTERRUPTION

- Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus or computer attack, including the voluntary shutdown of systems to minimize the business impact of the event.

DEPENDENT BUSINESS INTERRUPTION

- Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies on to run their business.

SYSTEM FAILURE

- Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional, and unplanned interruption of an insured's computer system.

REPUTATIONAL HARM

- Coverage for lost business income that occurs as a result of damage to a business' reputation when an actual or potential cyber event becomes public.

Industry Updates

Reviewing & Preparing

Review: Other Insurance Risks & Updates

- Business Income Coverage for COVID-19 losses
- Liability for COVID-19: What if...
 - Sued?
 - Sickness?
 - Other
- Employment Practices Liability
 - Include 3rd party coverage
 - Include Wage & Hour Violation Defe

Prepare: Insurance Marketplace Outlook

- Not all accounts are having issues or seeing significant rate increases
- Loss frequency or severity
- Large fleets or heavy trucks
- Umbrella capacity: \$10 million or more
- Builders Risk: Frame Projects

Questions?



Joe Urquhart, CPCU, CRIS, Vice President

✉ 614-453-4410 | jurquhart@oh-ins.com

in www.linkedin.com/in/joeurquhart/

Overmyer Hall Associates

Business Insurance | Surety | Home & Auto

🔗 www.oh-ins.com

in @OvermyerHallAssociates

f @OvermyerHall





SALT ISSUES FOR THE CONSTRUCTION INDUSTRY

PRESENTERS



Joe Popp, JD, LL.M.
Principal, Director of SALT Services



Sarah Sparks, EA, CP
Senior Associate

General Agenda

- COVID Phase 1 and Phase 2 Government Responses
- Economic Nexus – an area of continuing concern
- Detailed Discussions
 - Manufacturing Exemption – opportunity and pitfall
 - Municipal Tax Withholding for Transient Workers

COVID Impacts

- Phase 1 government responses are underway or completed
 - PPP
 - Stimulus checks
 - Enhanced unemployment
 - Delays to many filings and payments
 - State level holds on controversy work
 - Prioritization of refund request reviews

COVID Impacts

- Phase 2 government responses on the horizon
 - Due to proximity of the election, uncertain if second wave of federal stimulus behavior will occur before January.
 - Phase 2 is mainly revenue raising in nature
 - New Tax types – gross receipts?
 - Increased discovery, targeting out of state non-compliance
 - Removal of discretionary penalty relief
 - Increased use of “database” discovery (1099s, other state data).
 - Reduction in planned spending for important but non essential projects

SD wins *SD v. Wayfair*

- U.S. Supreme Court overruled old cases:
 - *Quill v N.D.*
 - *National Bellas Hess v. Dept of Revenue of IL*
- Held for South Dakota, upholding their economic sales tax nexus standard.
- Substantial Virtual Nexus
 - \$100,000 or 200 transactions in a state annually
- States have run wild implementing many different versions of this. **Almost every states with a sales tax has adopted economic nexus.**

Er...does this impact construction contractors?

- Usually, *you* are present in places where you have sales.
- YOU already have nexus.
- BUT....what about your vendors?

Example

- Non-Ohio vendor has sold you lots of stuff. They haven't charged you tax.
- YOU owe the tax. Maybe you paid it maybe you didn't.
- They ask you for the tax. What will you do?
 - Pay it
 - Refuse to pay it (they may disclose you to the state)
 - Pay it again (they don't accept your use tax filing as proof)
 - Give an exemption certificate (does that apply to you?)

Case Study: Construction Contractors & Manufacturers

- General Contractor won a bid with a large manufacturer to build a new manufacturing facility in Ohio.
- General contractor provided some asphalt & concrete construction contract services directly to manufacturing customer.
- Additional subcontractors were hired by General Contractor to supply other services like electrical, plumbing, framing, drywall, roofing, flooring, and HVAC.
- Additional vendors used by General Contractor included suppliers of furniture, signage, and manufacturing equipment, and installers of manufacturing equipment.

Case Study: Construction Contractors & Manufacturers (cont.)

- We assisted the General Contractor by providing the following services:
 - Reviewed the General Contractor's invoices to the manufacturing customer and blueprints of the project to determine manufacturing process beginning and end and what purchases fell into that process.
 - Provided General Contractor with determinations of which items being sold to manufacturing customer were exempt from sales tax and which were taxable.
 - Obtained a manufacturing exemption certificate from the manufacturing customer to provide to General Contractor for their purchases of manufacturing equipment & manufacturing equipment install services from vendors and subcontractors.
 - Provided General Contractor with completed resale certificate to give to their vendors for manufacturing equipment and business fixture purchases.

Case Study: Construction Contractors & Manufacturers (cont.) – End Results

- We helped the General Contractor save \$\$\$ on purchases from their vendors and subcontractors.
- General Contractor now has some guidance on when to pay sales tax and when not to pay sales tax so they can win future bids with lower costs.

Ohio Payroll & Transient Employees

- OK, sourcing employees' wages for payroll tax withholding for contract jobs with a single, fixed location is easy.
- But how do we know what city to withhold for when we have employees that do jobs all over Ohio?

Ohio Payroll & Transient Employees (cont.)

- Ohio's basic rule:
 - You need to withhold payroll taxes, somewhere, for every day an employee works.
 - Only one location can be counted as the city in which an employee worked each day, even if they work in multiple cities in a day.
- The easiest way to source wages to a city is if there is a normal "report to work location."

Ohio Payroll & Transient Employees (cont.)

- That's great, but my employees always work in 2 or more different Ohio cities each day. Is there any guidance on what city to start withholding for first and then when I need to switch to start withholding for other cities?
- Yes! We recommend using one of the three following sourcing methodologies for wages to determine your employees' "host city" and then when to start withholding for another city or cities:

Ohio Payroll & Transient Employees (cont.)

- Based on the prior year, determine in which city each employee spent the most time. Withhold for that city's tax for those employees unless and until you trigger the item in the bullet point below. You could call this their "host city."
 - After an employee has spent 20 days in a city, for the 21st day and every day thereafter start withholding on that city's tax for that employee when they work in that city. You would of course stop withholding on the "host city" above for the days you're withholding for this other city.

Ohio Payroll & Transient Employees (cont.)

- Based on the prior month or prior few months (if you don't have good data from last year), determine in which city each employee spent the most time. Withhold for that city's tax for those employees unless and until you trigger the item in the bullet point below. Again, this would be the employee's "host city" for this option.
 - After an employee has spent 20 days in a city, for the 21st day and every day thereafter start withholding on that city's tax for that employee when they work in that city. You would of course stop withholding on the "host city" above for the days you're withholding for this other city.

Ohio Payroll & Transient Employees (cont.)

- Based off of your reasonable estimation of where each employee works, determine in which city each employee spent the most time. Withhold for that city's tax for those employees unless and until you trigger the item in the bullet point below. Again, this would be the employee's "host city" for this option, just like in the previous options.
 - After an employee has spent 20 days in a city, for the 21st day and every day thereafter start withholding on that city's tax for that employee when they work in that city. You would of course stop withholding on the "host city" above for the days you're withholding for this other city.

To Do List Questions

- Where do you have nexus? Are you filing in those places?
- How are you managing the difference between real property and tangible property status job or portions of jobs?
- How are you documenting exemptions?
- How are you tracking use tax on items you may buy exempt?
- What software or procedures do you have in place to assist you in bidding on jobs, collecting exemption certificates or tax, and defending a possible future Ohio Tax audit?
- If buying or selling either most of the business assets of another company or the company itself, have you considered any latent SALT issues?
- For transient workers, are you always withholding city income taxes for every day they do work?

QUESTIONS?



Joe Popp, JD, LL.M.
Principal, Director of SALT Services
Joseph.Popp@reacpa.com
614-923-6577



Sarah Sparks, EA, CP
Senior Associate
Sarah.Sparks@reacpa.com
614-923-6592

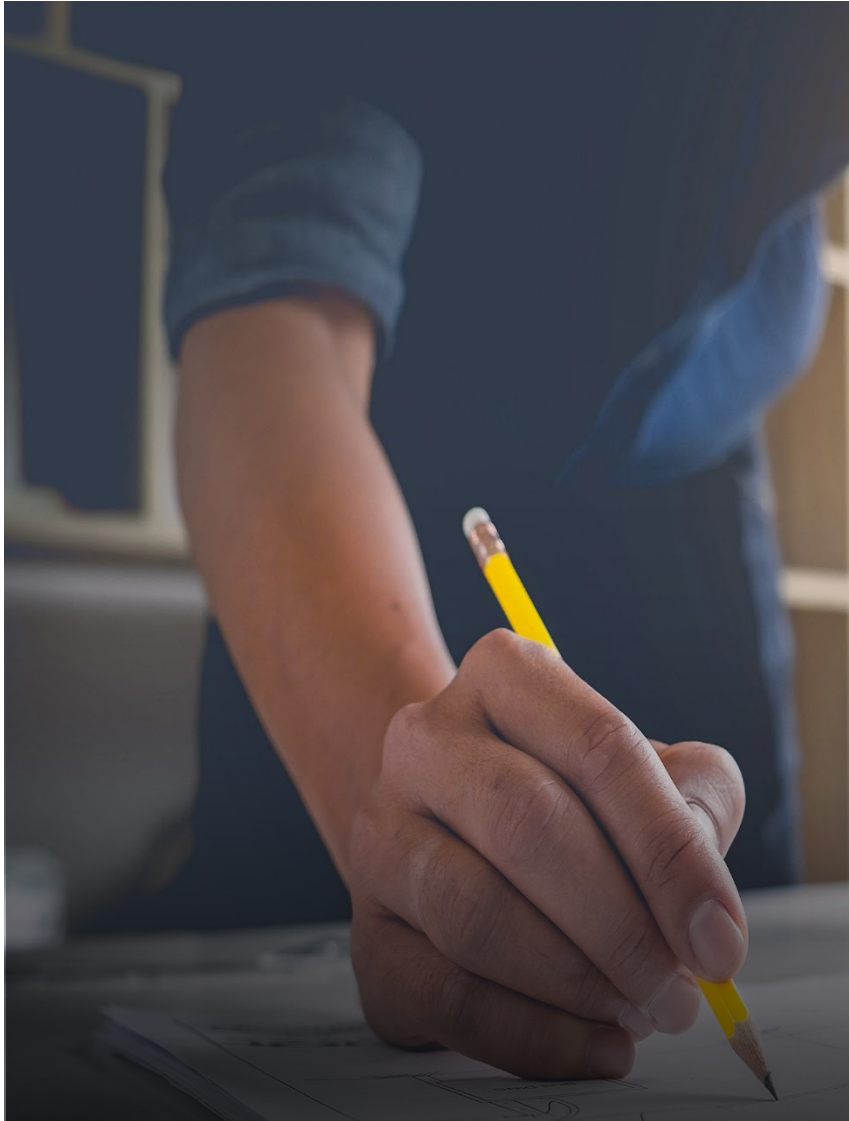


CONTRACT RISK

PRESENTER



J. Thomas Nocar
Senior Attorney



Q:
**WHAT'S THE #1
WAY TO AVOID
RISK ON A
JOBSITE?**



A: KNOW YOUR CONTRACT



TOP 10 TERMS FOR A SUCCESSFUL CONSTRUCTION PROJECT

HONORABLE MENTIONS



- Contract Entity
- Liquidated Damages
 - Difficult to calculate otherwise?
 - Reasonable and Proportional
- Termination
 - For cause
 - For convenience
- Prevailing Wage Rates

10. Attached Exhibits

Your proposal

GC contract (flow down)

Schedule

Drawings and specifications

Many others

LIST OF ATTACHMENTS AND SCHEDULES

ATTACHMENT A	Scope of Work and Addendums
SCHEDULE A-1	Scope of Work
SCHEDULE A-2	Addendum 1
SCHEDULE A-3	Addendum 2
ATTACHMENT B	Drawings and Specifications
SCHEDULE B-1	Drawings
SCHEDULE B-2	Specifications
ATTACHMENT C	Contractor's Compensation Schedule
ATTACHMENT D	Project Schedule
ATTACHMENT E	Delay Liquidated Damages Schedule
ATTACHMENT F	Approved Subcontractors List
ATTACHMENT G	Lien and Claim Waiver Forms
SCHEDULE G-1	Contractor's Interim Lien and Claim Waiver
SCHEDULE G-2	Subcontractor's Interim Lien and Claim Waiver
SCHEDULE G-3	Contractor's Final Lien and Claim Waiver
SCHEDULE G-4	Subcontractor's Final Lien and Claim Waiver
ATTACHMENT H	Form of Mechanical Completion Certificate
ATTACHMENT I	Form of Final Completion Certificate
ATTACHMENT J	Insurance
ATTACHMENT K	Right-of-Way and Access
SCHEDULE K-1	Right-of-Way Provisions
SCHEDULE K-2	Haul Route
ATTACHMENT L	Owner Permits
ATTACHMENT M	Contractor Permits
ATTACHMENT N	Owner-Furnished Items and Services

9. Attorney Fees & Costs

Allowed?

One party only

Prevailing party

Conditions to collect

8. Dispute Resolution

- Negotiation
- Mediation
- Arbitration
- Litigation
- Venue
- Choice of law

7. Notice of Claims

Requirements of notice

Written notice

Timing of notice

Waiver

6. Insurance

- Risk tolerance
 - Limits
 - Coverage
- Insurable Event
- Liability for Non-covered events
- Bond Requirement

5. Indemnity

One party agrees to pay the losses of another party



INDEMNITY

- Limits risk of liability
- Mutually
- Apply to work controlled
- Narrow scope - concise
- Omit acts of indemnitee
- Legal costs included?

4. Change Orders

CO Process

Change Directives

Lump Sum or Itemized Cost Plus

Required Backup

Approval

Payment

3. Schedules

Clear

Reasonable durations

Time frames as bid

Integrates with other work

2. Scope of Work

Clear

Concise

Complete

Correct

Coordinated



SCOPE OF WORK

- Temporary utilities
- Crane or hoist
- Material laydown area
- Parking
- Matches bid
- Qualifications/Exclusions
- Access to work
- Special site provisions

1. Payment

Initial Deposits

Progress Pay

Milestone Pay

Stored Materials

Retainage

Final Payment

Invoicing requirements

Top 10 Contract Terms

1. Payment
2. Scope of Work
3. Schedule
4. Change Orders
5. Indemnity
6. Insurance
7. Notice of Claims
8. Dispute Resolution
9. Attorney Fees & Legal Costs
10. Attachments

DISCLAIMER

Porter Wright Morris & Arthur LLP offers these materials for general information purposes only. The content of these materials is not intended as legal advice for any purpose, and you should not consider it as such advice or as legal opinion on any matters. This content does not necessarily reflect the views of the firm as to any particular matter or those of its clients.

The information provided herein is subject to change without notice, and you may not rely upon any such information with regard to a particular matter or set of facts. Further, the use of these materials does not create, and is not intended to create, any attorney-client relationship between you and Porter Wright Morris & Arthur LLP or any individual lawyer in the firm. Use of these materials is at your own risk, and the materials are provided without warranty of any kind. We make no warranties of any kind regarding the accuracy or completeness of any information in these materials, and we make no representations regarding whether such information is reliable, up-to-date, or applicable to any particular situation. Porter Wright Morris & Arthur LLP expressly disclaims all liability for actions taken or not taken based on any or all of the contents of materials, or for any damages resulting from your viewing and use thereof.

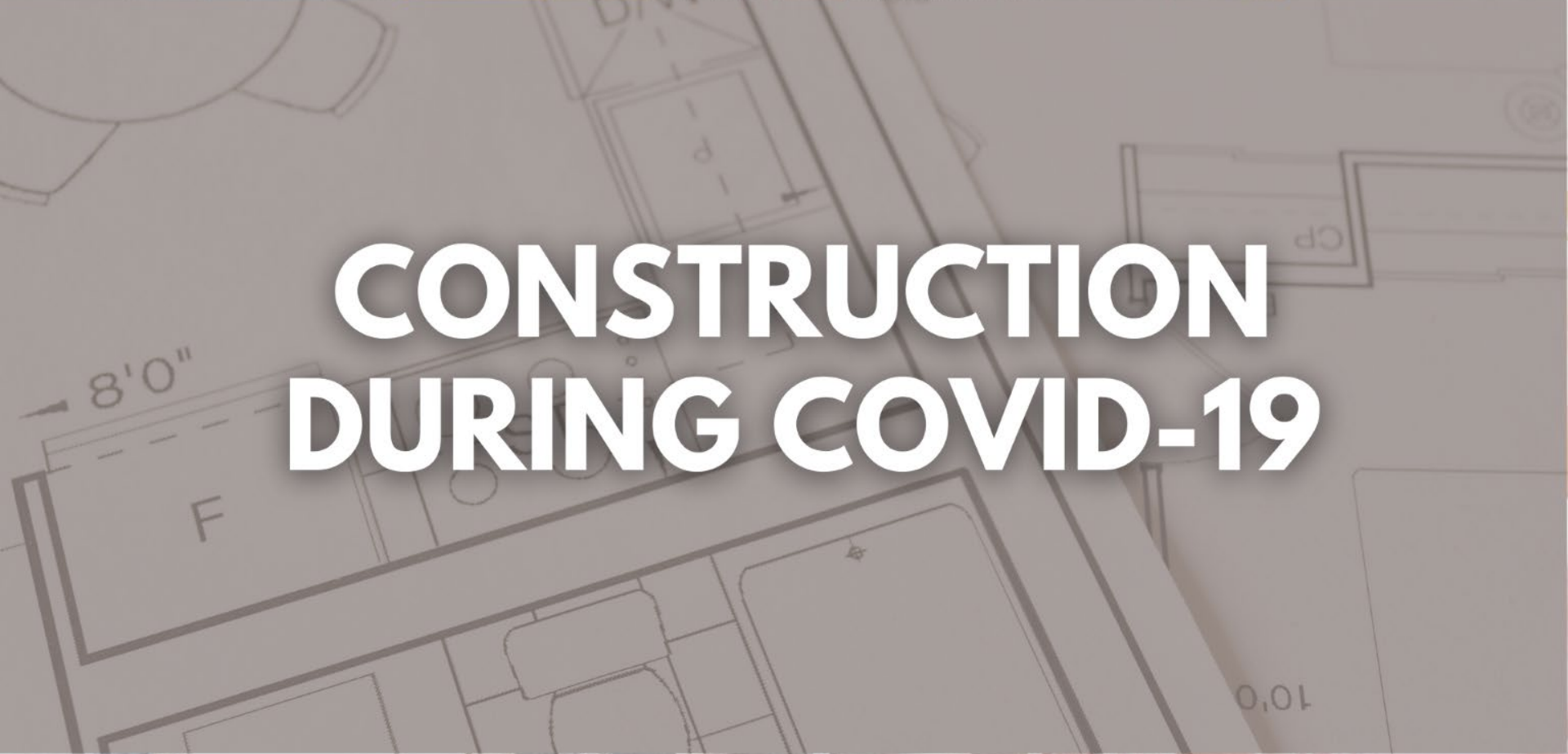
QUESTIONS?



J. Thomas Nocar
Senior Attorney
tnocar@porterwright.com
614.227.2031
www.porterwright.com



CONSTRUCTION DURING COVID-19





CONSTRUCTION
DURING COVID-19

WELCOME

TRAVIS
SPAGNOLO,
MBA, CSP

614.890.0800 ext. 205

tcspagnolo@safex.us



OBJECTIVES

At the end of this session attendees will be able to:

1. State respiratory protection requirements;
2. Communicate potential methods to increase sanitation and limit COVID spread on construction sites;
3. Identify potential tasks with increased COVID risks;
4. Describe actions to take when a positive case is discovered.

COVID-19 AND VIRUS TRANSMISSION

Primary transmission is through respiratory droplets. Surface to touch transmission is possible, but not as likely.





WHICH OF THESE BEST PREVENTS VIRUS SPREAD?





WHICH IS CONSIDERED A FORM OF PPE?



USE OF RESPIRATORS

Voluntary Use

- Employee is not required to wear the respirator by a supervisor or their employer.
- No fit test required.
- Employee must sign Appendix D of 1910.134.
- Only filtering facepiece N95 permitted to be worn voluntarily.
- Must be NIOSH approved.

Mandatory Use

- Employee required to wear respirator by a supervisor or employer.
- Employer provides respirator.
- Employee must be fit tested, medically cleared, and trained to wear the respirator.
- Company must have a written respiratory protection program.
- Must be NIOSH approved.

CONTRACTOR RECOMMENDATIONS



Develop a plan AND enforce it.



Continue planning and budgeting for COVID-19.



Ensure contract language includes subcontractor requirements and expectations.



Know your response for when you have a positive case.

ASSESSING RISK

Different trades, tasks, and jobsites will all present different risks:

- Inside or outside?
- What tasks are being performed?
- How many people are in the area?



MITIGATING RISK AND RECOMMENDED ACTIONS

Staggered start/stop
times

Increased hand
sanitizing and hand
washing stations

Regular cleaning and
disinfecting of
frequently used tools
and equipment

Increase cleaning
schedule of restrooms
and frequently touched
objects (door handles,
handrails, etc.)



Provide personal items such as harnesses, face shields, welding hoods, etc., to employees to use individually



Conduct project meetings virtually



Ask employees to take breaks and eat lunch in their cars

MITIGATING RISK AND RECOMMENDED ACTIONS

Remain calm.

Work with attorneys to craft a letter indicating that there has been a positive case.

You are not permitted to reveal the identify of the individual who has tested positive.

Local health departments are responsible for contact tracing.

It is up to the employer to determine next steps such as shutting project down or performing a deep clean.

If exposure can be found or proven at work, the illness becomes an OSHA recordable.

POSITIVE
CASE



QUESTIONS? |



Contact us

Central Ohio's Business Health,
Safety and Environmental
Consultants since 1992.



facebook.com/safex.us



[Linkedin.com/company/safex-inc](https://linkedin.com/company/safex-inc)



140 N. Otterbein Ave.
Westerville, Ohio 43081



614.890.0800

CONTACT INFORMATION



Doug Houser
Doug.Houser@reacpa.com
(614) 314-5937



Joe Popp
Joseph.Popp@reacpa.com
614-923-6577



Joe Urquhart
jurquhart@oh-ins.com
614-453-4410



Scott Bechtel
Scott.Bechtels@reacpa.com
(614) 923-6547



Sarah Sparks
Sarah.Sparks@reacpa.com
614-923-6592



J. Thomas Nocar
tnocar@porterwright.com
614.227.2031



Shawn Richardson
Shawn.Richardson@reacpa.com
(234) 249-3478



Travis Spagnolo
tcsagnolo@safex.us