

Staying “3 Steps Ahead” of the Cyber Construction Curve

January 2020 | AGC

Greg Perruzzi
VP, Enterprise Risk Manager | Sphere

INTRODUCTION

- ▶ **Risk Manager's Perspective:** Unique Business Model/Unique Market/Unique Risk
- ▶ **Enterprise Approach:** Develop a Solution with 3 Prongs
- ▶ **Realities & Challenges:** Opportunity

CYBER INSURANCE RISK 101 - covered?

Cyber-insurance protects businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.

- ▶ **Traditionally, the coverage is comprised of 2 parts:**

- ▶ First Party Coverage (Property/Expenses/Fines/Income Loss & Crisis Management Services)
- ▶ Third Party Liability (Financial and Economical losses)

- ▶ **Cyber Coverage pivots off of 2 basic assumptions:**

- ▶ Event Trigger: There is a form of breach, failure, attack, threat or hacking resulting in an “event”
- ▶ There is a subsequent financial or economic loss suffered as a result of the “event”

CYBER INSURANCE RISK 101 - not covered?

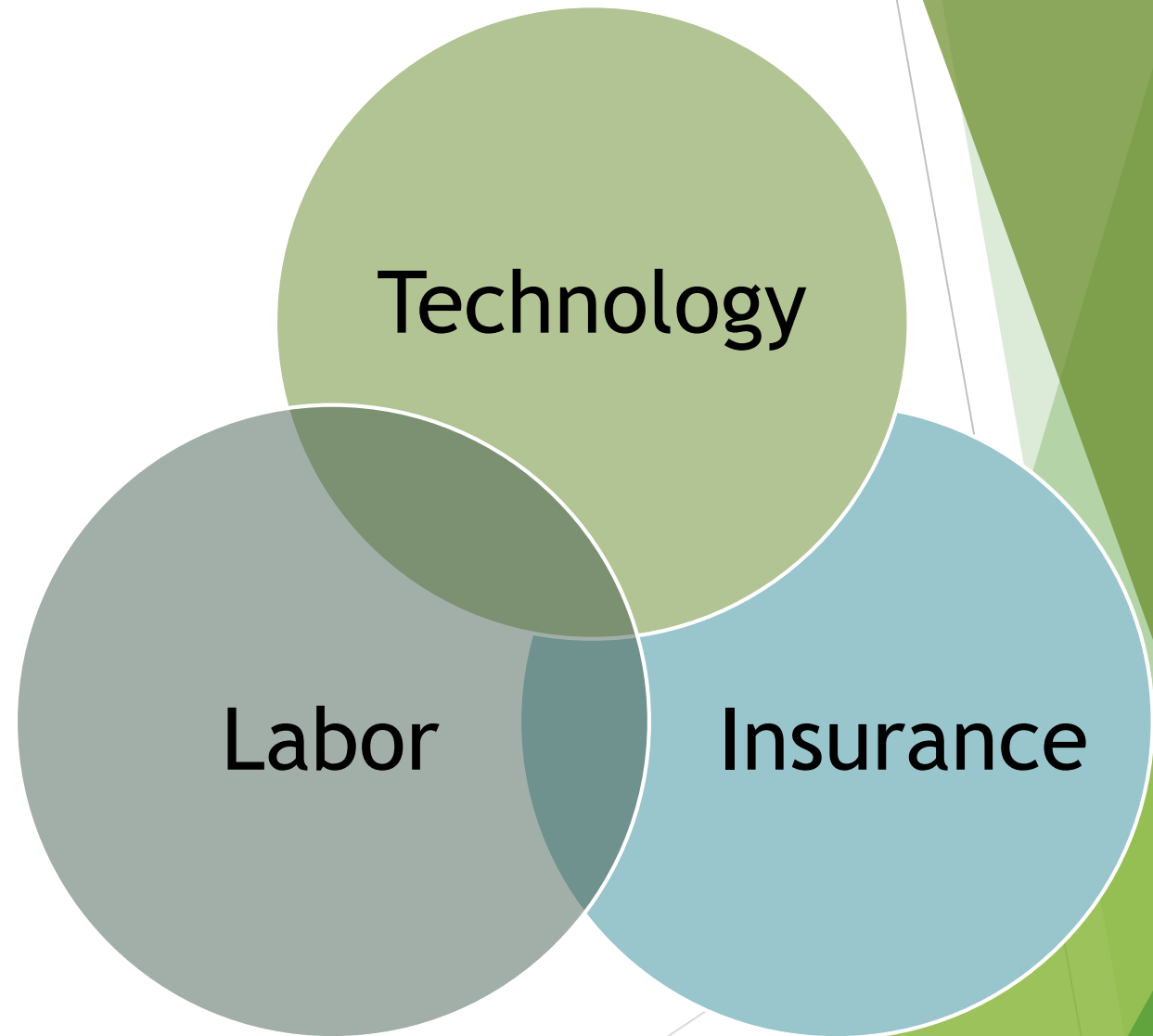
► There is a GAP....

<u>Coverage Matrix:</u>	<u>1st Party</u>	<u>3rd Party</u>	<u>Cyber Exclusion</u>
Professional Errors/Omissions - Economic Damages	X	X	
General Liability Bodily Injury/Property Damage	-	X	X
Property/Builders Risk	X	-	
Cyber Liability	X	X	



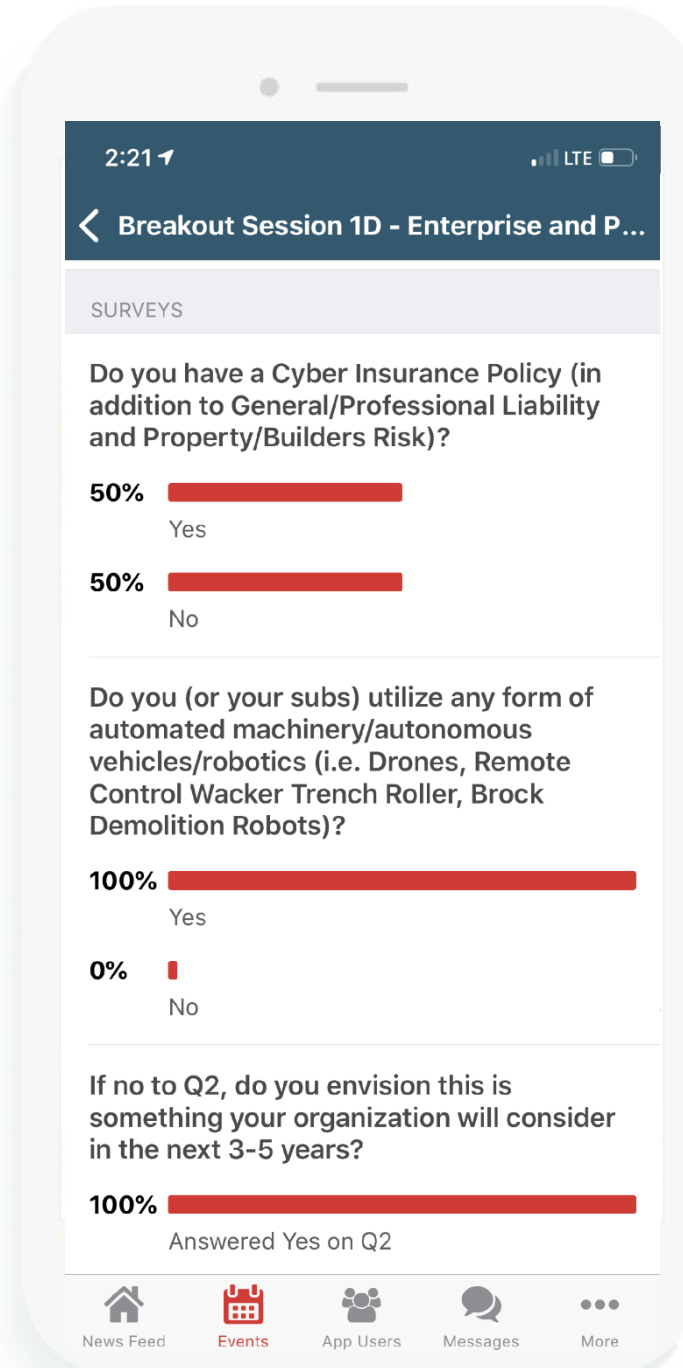
RISK CONVERGENCE?

- ▶ Construction Tech Investment
- ▶ Approach to Skilled Labor
- ▶ Insurance Market Hardening

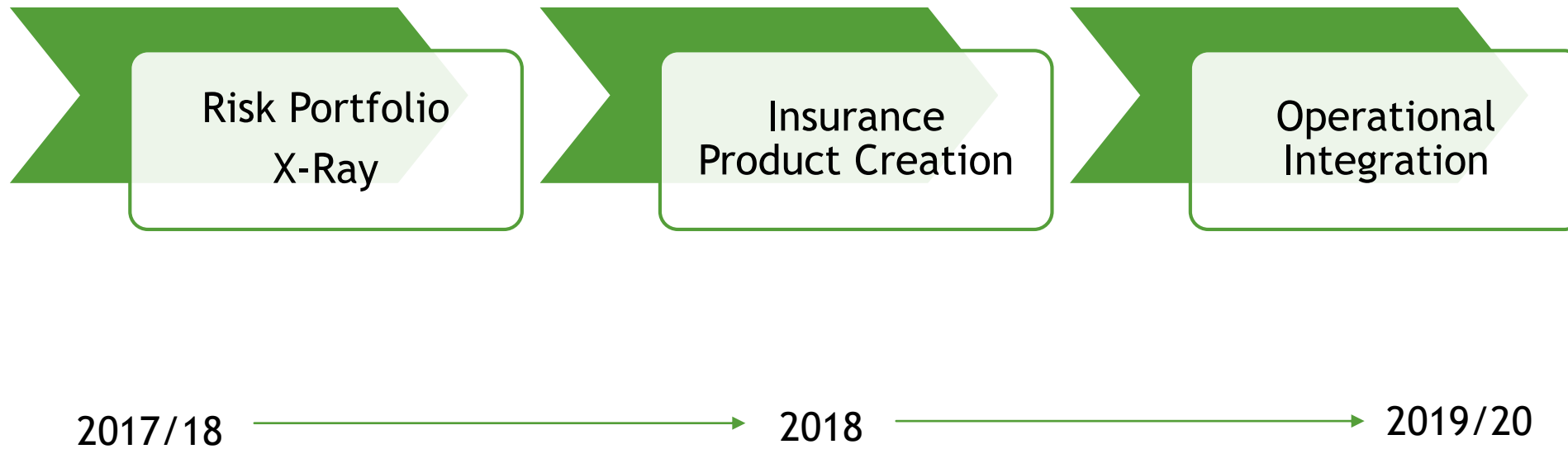


LIVE SURVEY

- ▶ RM attendees to vote **Y/N** on following questions and we will check in on your answers in real-time...



ENTERPRISE APPROACH - 3 Steps



ENTERPRISE APPROACH



Risk Portfolio
X-Ray

- ▶ **Corporate Level Engagement (5 months):**
 - ▶ Categorize 1st/3rd Party Risk into Quadrants
 - ▶ Integrate CTO and Claims Manager into evaluation and decision making process
 - ▶ Leverage brokerage partners within cross sectional LOB's (Cyber)

RISK QUADRANTS

- ▶ Could a cyber event apply in each?
- ▶ How do we categorize priorities?
- ▶ Optimize insurance portfolio approach?

	First Party Impacts	Third Party Impacts
Financial Impacts	<ul style="list-style-type: none">• Crisis response costs: forensics, notifications, credit monitoring• Legal expenses: advice and regulatory filings• Business Interruption loss from network or computer outages, including cloud• Theft of funds, monies, or securities• Cost of restoring lost data• Cyber extortion expenses• Value of stolen intellectual property	<ul style="list-style-type: none">• Consequential lost income• Restoration expenses• Legal defense• Civil fines and penalties• Shareholder losses
Tangible Impacts	<ul style="list-style-type: none">• Mechanical breakdown of your equipment• Destruction or damage to your facilities or other property• Environmental cleanup of your property• Lost income from physical damage to your (or dependent) equipment or facilities (business interruption)• Bodily injury to your employees	<ul style="list-style-type: none">• Bodily injury to others• Damage to property of others• Mechanical breakdown of others' equipment• Environmental cleanup of others' property• Product liability• Product recall expenses

CLAIMS SCENARIO

► Example Situation:

Who: A hacker with a vested interest in disrupting a project or developer's project compromises all operating/electronic data systems (i.e. computer controlled crane). The crane malfunctions and turns into a neighboring building while sending debris into the street and project.

What: The project's Cyber attack causes damage to a neighboring building while injuring workers and a pedestrian. In addition, there is resultant delay to the project, including damage to the crane itself.

How: A targeted cyber-attack from this hacker breaks through the cranes automation software-driven systems and remotely takes control of its operations.

CLAIMS SCENARIO

► Impact:

- The Owner expects his contractual indemnity and insurance rights honored.
- The Owner also expects the crane to be replaced immediately.
- A pedestrian is injured and taken away in an ambulance.
- The NYDOB shuts the project down under a full work stop order.

ENTERPRISE APPROACH



Insurance
Product Creation

- ▶ **Robust Cyber “Construction” Program Strategy**
 - ▶ 3 Months - Develop Specifications
 - ▶ Coverage/Limit/Service
 - ▶ 1.5 Months - Schedule Carrier Presentations
 - ▶ Business Model Explanation
 - ▶ Risk Management Philosophy
 - ▶ 1.5 Months - Drive Negotiations/Quote Leveling/Bind
 - ▶ Robust Cyber Form (Integrated w Construction)
 - ▶ Affirmative 3rd Party BI/PD (Occurrence Limits)
 - ▶ ALAE (separate dedicated defense limits)
 - ▶ Conditioned to address Enterprise Needs

Claims Scenario/Coverage Confirmed

► Example Situation

1. Builder's Risk (two types): NOT COVERED

Builder's Risk - direct physical loss or damage to Tangible Property and Software/ Operating Systems are Not covered.

2. General Liability (two types): NOT COVERED


CGL or Wrap-Up policies with new ISO exclusionary language on Cyber or Electronic Data including.

- **ISO CG 21 07 05 14** : excludes Bodily Injury AND Property Damage
- **ISO CG 21 06 05 14** : contains identical language, but only **excludes Property Damage**

3. Cyber Liability: **CYCON COVERED**

- **Contingent Bodily Injury and Property Damage sub-limits due to cyber events**
- Regulatory expansion for inquiries and defense/ fines and penalties - particularly as it applies to employee information or OSHA
- Paying any service credits or contractual penalties that an Insured may be contractually obligated to pay
- Additional Expenses - services, premises, employing contract staff, or overtime costs of employees

ENTERPRISE APPROACH



Operational
Integration

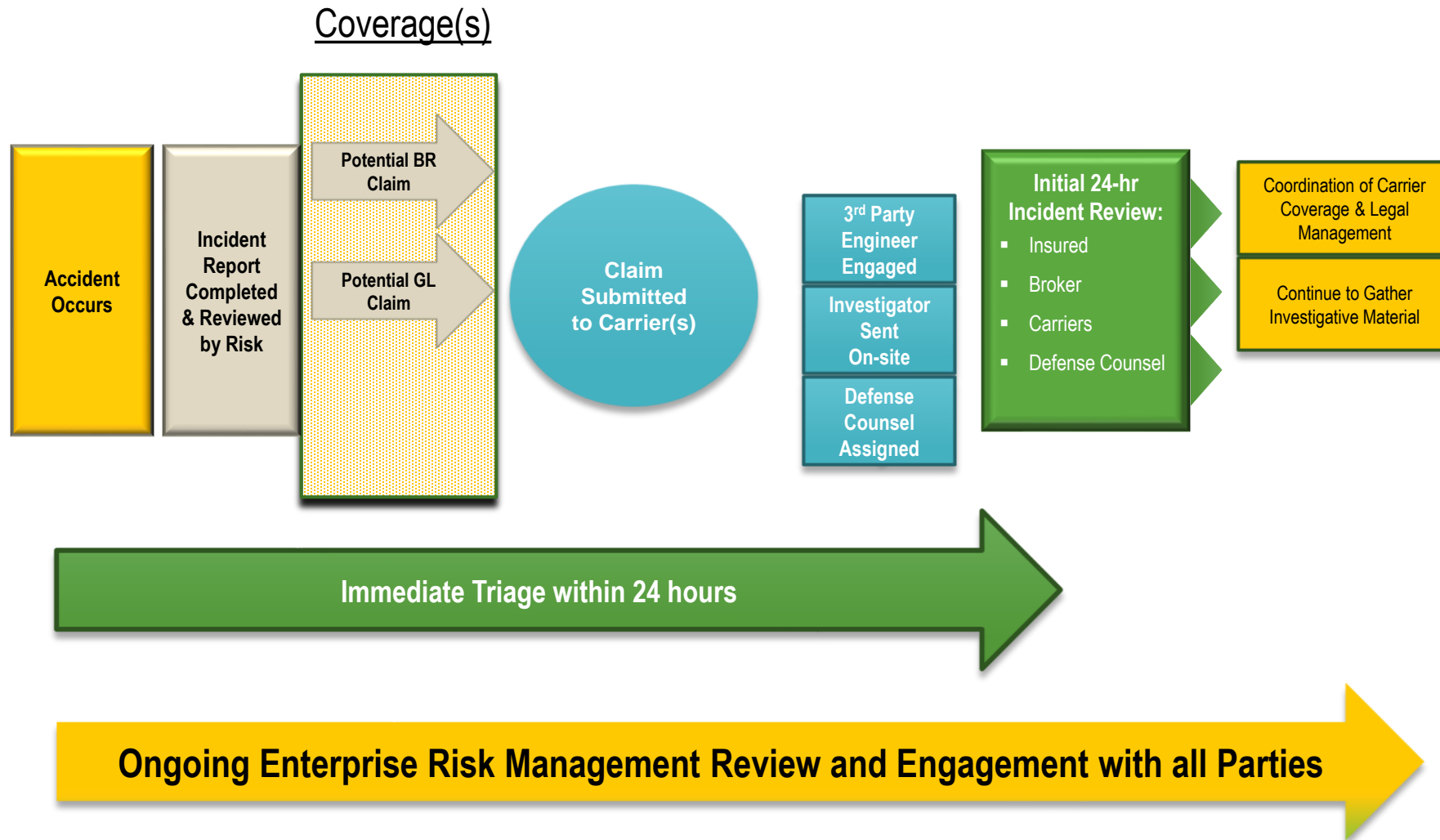
- ▶ **Prudent Insurance / Risk Management Steps (Ongoing..)**
 - ▶ Corporate Level:
 - ▶ Integrated Cyber Construction Incident Management
 - ▶ Aligned Enterprise BCP/DR/Crisis Management
 - ▶ Project Operations Level:
 - ▶ Vet Cyber Risk Exposure (i.e. Geography/Project Scope/ Subcontractor Type/Owner)
 - ▶ Conduct stress tests on incident response plan, ID coverage triggers (1st party/3rd party)

CONSTRUCTION INCIDENT CONSIDERATIONS

- 1 You may not know if there is a cyber element at the time of the incident - immediate response will follow standard BI / PD protocols.
- 2 Protocol must include a cyber check.
- 3 Once it's determined that there may be a cyber element your plan should incorporate 2 questions:
 - ▶ What do I need to do to preserve coverage under my cyber policy?
 - ▶ What Auxiliary benefits does my cyber policy provide to help manage and mitigate the loss?

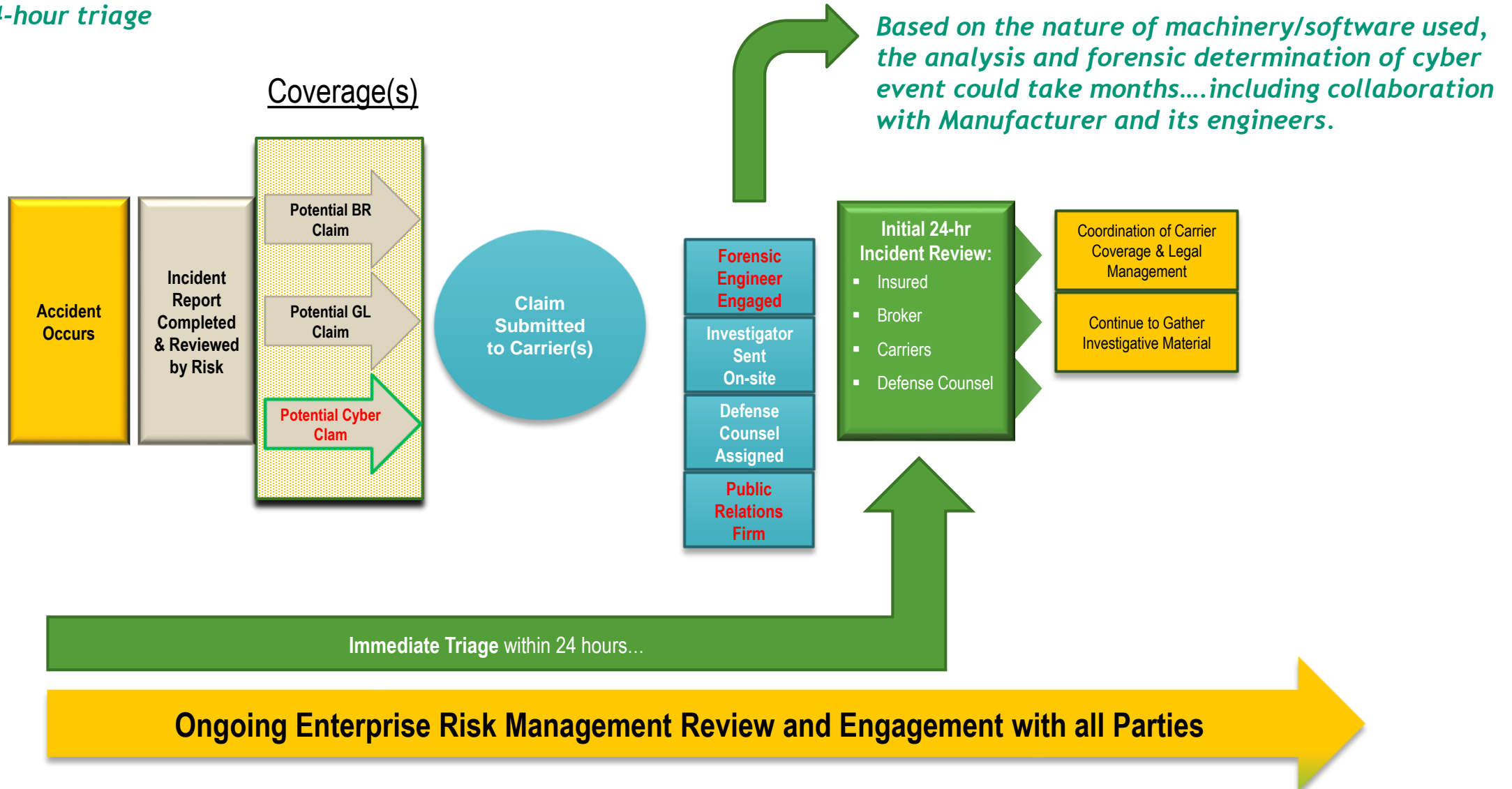
CONSTRUCTION INCIDENT RESPONSE

**Sample 24-hour triage*



CYBER CONSTRUCTION INCIDENT RESPONSE

**Sample 24-hour triage*



EVALUATING RISK SERVICE PARTNERS

- ▶ Panel/Legal Counsel - Cyber / GL “Hybrid”
- ▶ Investigation Firms
- ▶ Forensic Engineering Firms
- ▶ Public Relations
- ▶ IT service providers
- ▶ Claims /TPA Management
- ▶ Crisis Management Firms



CyberCon Program

Litigation Management Meeting Intro (Lewis Brisbois)

10/23/19

Basic introduction - Program

- Sphere Risk / LB Legal Team(s)
- CyberCon Program – 60ft Level
 - Coverage Form
- Current NAS/Willis Relationship and Synergy w Legal and Sphere
- Market Knowledge on CyberCon litigation?? Example Cases??

Today Focus – Claims and Litigation Management

- LB Interaction between GL and Cyber Partners
- Notice Triggers
- Claims and Investigatory Triage
 - GL v Cyber
 - Risk and IT v Operations
 - 3rd Party Vendors
- How do we enhance and build program that overlays w current GL Lit Mgt?

Next Steps

- Consensus on how Program and Lit Management is approved w NAS
- Additional Meetings and Planning
- Misc.

CRISIS MANAGEMENT PLAN / TABLE TOP



A person wearing a dark hoodie is shown from the side, typing on a laptop. The background is a dark blue screen filled with white text, resembling a computer terminal or a web page with code. The text includes various HTML tags and URLs, such as 'www.dingjue.cn' and 'templates/images/logo.jpg'. The overall atmosphere is technical and digital.



KEY TAKEAWAYS

- ▶ **Be Aware** - Project Cyber Construction Risk Profile Increasing
 - ▶ Investment in Construction Tech
 - ▶ Building LEAN/Labor Efficiency
 - ▶ AIA Insurance Requirements/Owner Requirements
- ▶ **Stay Proactive** - Enterprise Risk Management Approach Required
- ▶ **Balance Importance** - Insurance Coverage Solution & Operational Planning
- ▶ **Drive Carrier(s) Support and Product Solutions Opportunity**
 - ▶ Corporate Practice Program
 - ▶ Project Specific Program
 - ▶ Wrap Up Program (subcontractors/3rd party machine/equipment providers)

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

THANK YOU

January 2020 | AGC

Greg Perruzzi
VP, Enterprise Risk Manager | Sphere