1. What is a cyber risk?
2. What are the impacts to the public sector?
3. What can be done to protect your organizations?
71% of organizations said cyberattacks are still a “bit of a black box.”

“We struggle to understand how an attack would impact our organization beyond the obvious.”
Cyber and people underpin every part of modern life.
Interconnectivity helps everyone...
…until it doesn’t.

> 70 state and local governments affected by ransomware in 2019 so far

$3 trillion in economic losses by 2020

A single data breach could cost > $4 million on average
Public sector faces the same, **if not more**, systemic cyber risks as the private sector.
No longer a question of if but WHEN and HOW BAD
45% of municipalities attacked had populations < 50,000
24% had < 15,000
It gets worse.

- Fraud and theft of funds
- Disable critical systems and services
- Control of critical systems and services
- Cyber-physical attacks
Emerging cyber risks create multiple impacts – financial and reputational – *across multiple lines.*

If you don’t know what all the impacts are, are you protecting against **ALL** of them?
What is Silent/Non-affirmative coverage and how does it impact you?
How will cyber risks manifest in your organization?

Understand, measure, and manage every risk, not just the insurable ones.
A Call to Arms

- Trace your cyber footprint.
- Take stock of your organization, your assets, your goals.
- Ask the hard questions now – the public will not be kind post-event.

- Pick the meaningful metrics.
- Measure your risks ACROSS the organization – account for interdependencies and cascading risks and your constituents.

- Develop an integrated strategy that involves the entire organization, not just risk management.
- Leverage all available tools – integrate business continuity planning, cash reserves, security investments, insurance, etc.

- Lather, rinse, repeat.
QUESTIONS?
THANK YOU!