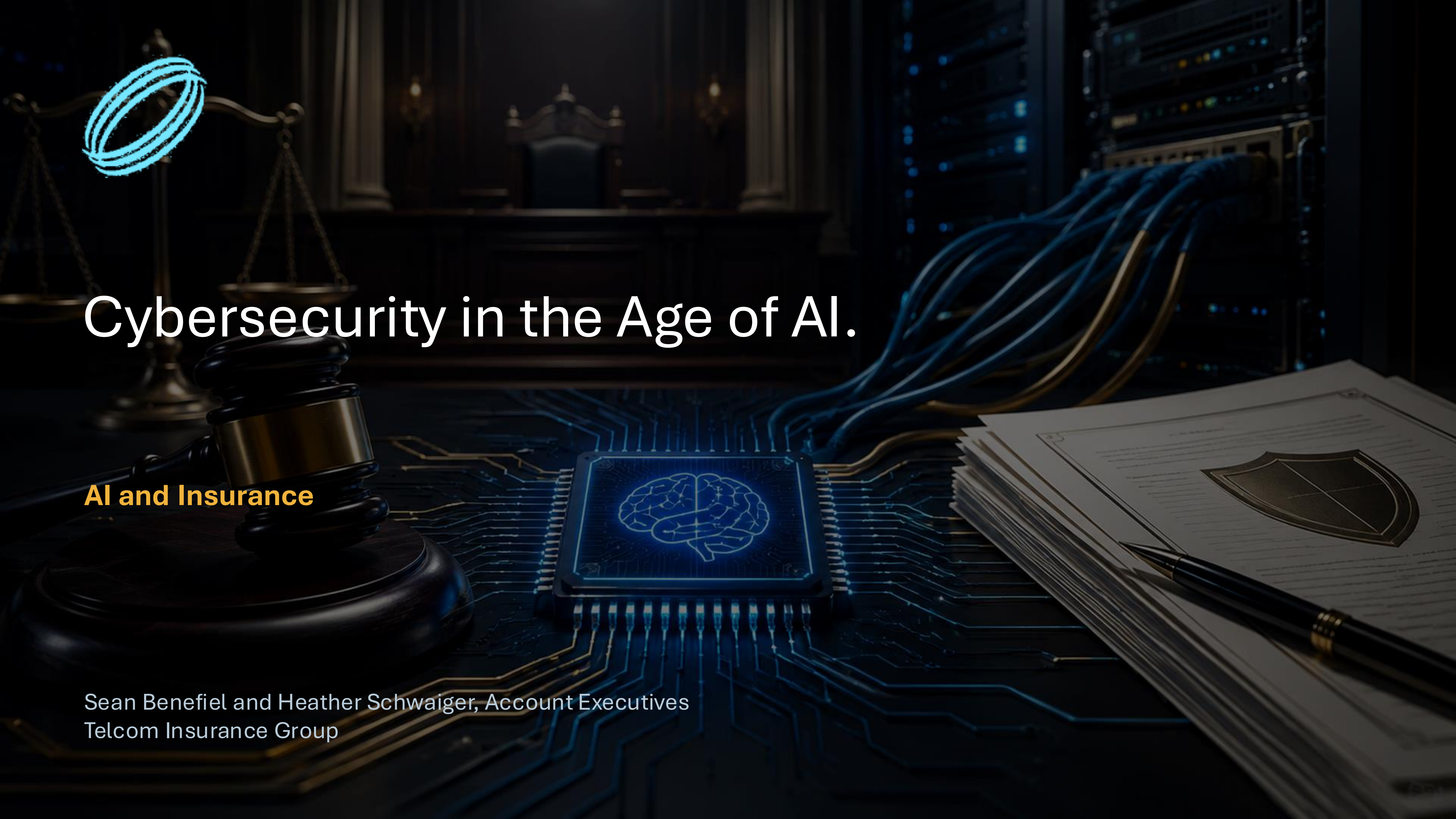

Cybersecurity in the Age of AI.

AI and Insurance

Sean Benefiel and Heather Schwaiger, Account Executives
Telcom Insurance Group

The simple message

AI does not remove the need for judgment.

The organization that can explain its human decisions will be more defensible, more compliant, and less risky.

> **AI does not remove judgment; rather, judgment on use becomes the first thing.**

AI creates risk when these things exist

That is the moment AI becomes a management risk.

1 It influences a decision

2 People rely on the output

3 A real person or regulator is affected

> **That is the moment AI becomes a risk to an organization.**

Where are there exposures

Analyzing and finding risk is step one to managing it.

- Privacy
- Inaccuracy
- Bias
- IP
- Deepfake fraud
- Operational disruption
- Physical injury or property damage

AI risk is not one policy. It is a fact pattern.

Why telecom leaders should care

A highly regulated and scrutinized industry that people's lives depend upon.

Telecom providers do not have to build the AI to be drawn into the claim.

They may transmit it, authenticate it, route it, host it, integrate it, automate it, or communicate through it.

> **Enablement can be enough for liability to exist.**

Case: AI-generated traffic

AI can be used to exploit networks, breaches, and for the use of the system.

$1M FCC settlement

Lingo Telecom settled with the FCC for $1 million and compliance obligations after spoofed AI-generated robocalls used voice cloning.

The liability issue is not only who created the message. It is who could have authenticated, monitored, blocked, or controlled the traffic.

> AI misuse moving across a network can become telecom liability.

Deepfake fraud changes the control

Virtual meetings are being used to trick employees.

**Verify the transaction,
not the face.**

In 2024, Arup lost $25 million to a deepfake scheme that tricked 15 employees, not just 1.

Commercial crime and cyber coverage both get tested.

Privacy and biometrics are different

"No breach" does not mean "no privacy related issue."

A biometric AI claim may not need a data breach.

Notice, consent, retention, and use limitations can create statutory exposure before anyone steals data.

> **People get very touchy about their likeness, voice, fingerprints, or similar things being collected.**

Bias is an enterprise risk

AI decided with a flawed algorithm isn't going to be accepted as an excuse.

Data may look harmless or neutral, but beneath the surface, it can violate protected traits.

The evidence question is simple:
Can you prove the model was tested, monitored, and, if need be, corrected?

> **Bias isn't just bad when it comes from a machine; the management that allowed it to exist is bad as well.**

When AI is somewhere beyond the screen

Bad advice used to create confusion. AI bad advice can create injury.

AI embedded in equipment, safety advice, infrastructure, maintenance, routing, or operational control can create bodily injury or property damage.

An autonomous car can fail to stop.
NOC monitoring AI doesn’t read a breakdown signal
When AI gives wrong consulting advice

Insurance responds to the trigger of injury

Name the consequence first.

The word “AI” does not determine coverage.

The trigger does: theft, breach, privacy invasion, error, misrepresentation, bodily injury, property damage, discrimination and employment action, media claim, or regulatory investigation.

- Property/Crime
- Cyber Breach
- Error and Omission
- General Liability
- Executive Liability
- Media Liability
- Personal Injury
- Regulatory Fine
- Intellectual Property

Gaps to watch

See if the real cost of coverage is greater than what is on the dec page.

AI exclusions
Algorithmic decision exclusions
TCPA / BIPA / statutory damages limits or exclusions
Regulatory fines exclusions
Vendor limitation-of-liability gaps
No coverage for pure service failure without physical damage
Director and Officer Coverage Terms and Exclusions

> Stress-test to see if risk bankrupts you before it actually does.

The governance loop

Governance is documented human judgment.

GOVERN — who owns the AI?

MAP — where is it used?

MEASURE — how can it fail?

MANAGE — who can stop or correct it?

> **Is there any means to transfer the risk, or has it been transferred to us?**

Vendor contracts matter

The black-box problem is often a contract problem.

Ask every AI vendor

- What data is used?
- What is logged?
- Who indemnifies?
- Who can shut it off?
- What and who’s insurance backs the promise?

> You would be amazed at what can be transferred in a contract

Monday morning checklist

Small discipline beats big surprise.

- Inventory AI tools.
- Assign employee owners.
- Identify high-impact decisions.
- Review vendor contracts.
- Test insurance scenarios.
- Create override, pause, and notice rules.

> An ounce of prevention is worth a pound of cure.

Attendee exercise

Coverage trigger or coverage trap?

AI is monitoring customer alarm systems, and it misses a break-in.

Deepfake video triggers a $1.8M wire transfer.

AI used by HR creates an algorithm for raises that uses gender.

Which policy do you review first?

Closing thought

Human oversight is not anti-innovation. It is what can make innovation less risky.

AI does not replace judgment.
It demands better judgment earlier.

> “The future will not belong to companies that remove humans from the process. It will belong to companies that put better human judgment at the beginning and end of the process.”

Thank you for attending!