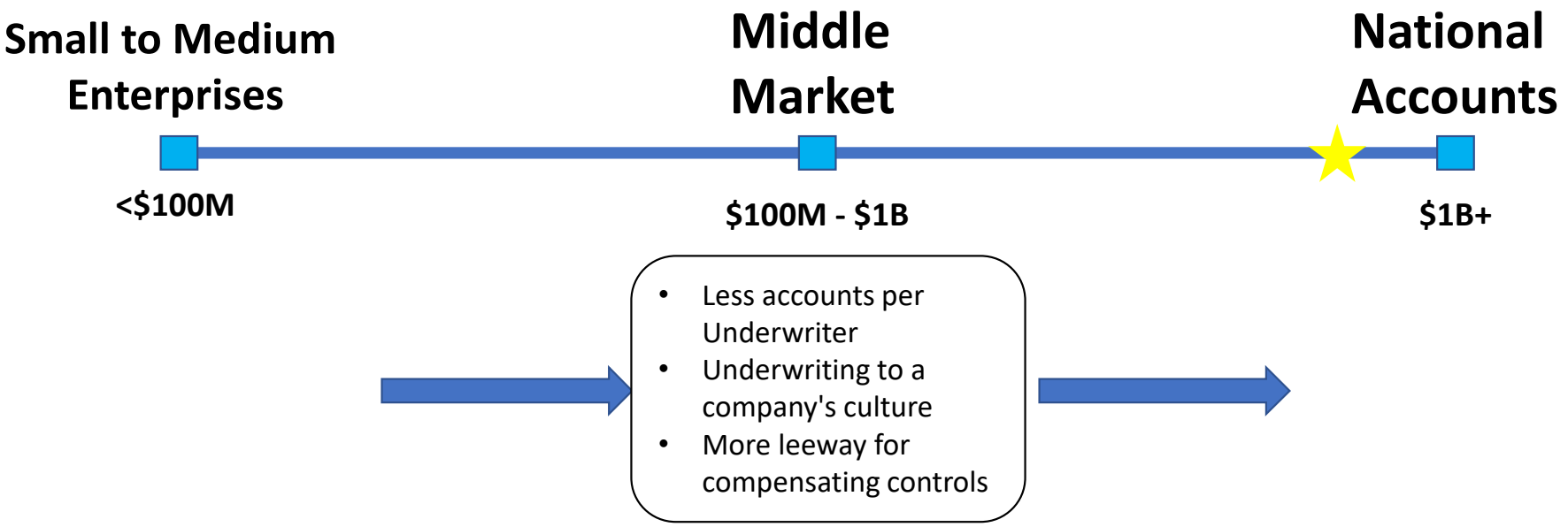
How Carriers Evaluate Cyber Risk

Connor Bowen, Underwriter

Berkshire Hathaway Specialty Insurance Appetite

Where we are positioned in the cyber insurance ecosystem



2020-2023

Then:

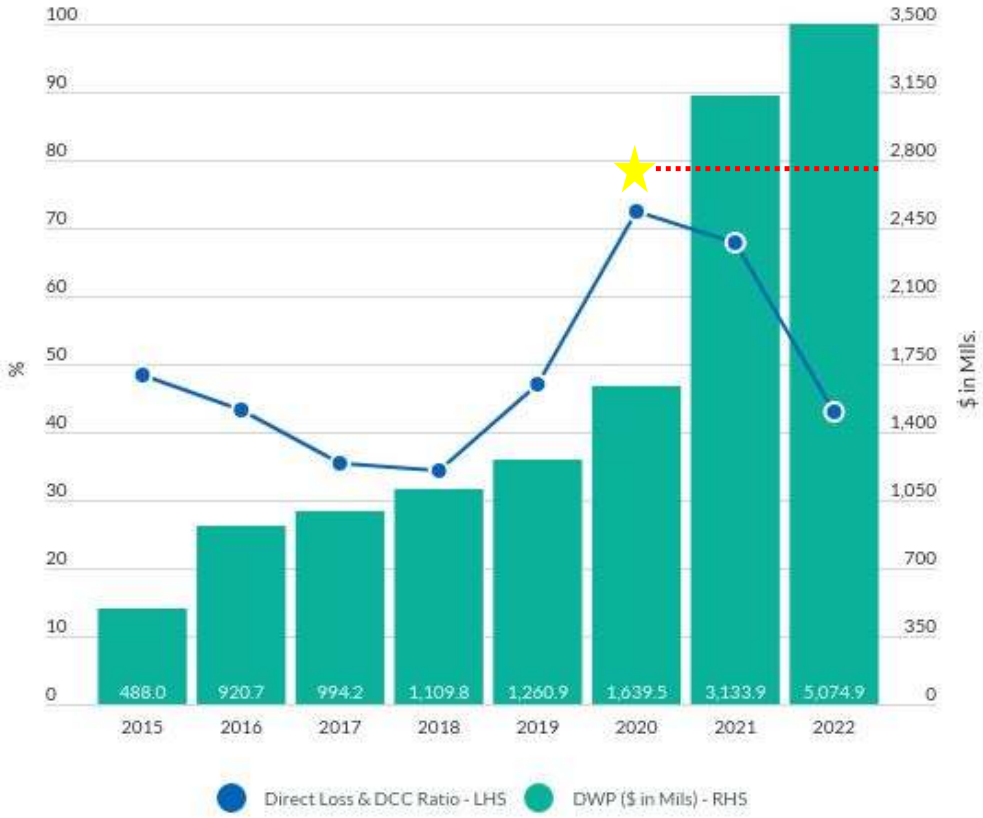
- Lower Premium
- Rigid underwriting
- Propensity towards declining submissions
- One of the first years with significant losses

Now

- Higher premium
- More knowledgeable underwriters
- Increased comfort with the risk
- Openness towards compensating controls

Standalone Cyber Risk Direct Loss & DCC Ratios

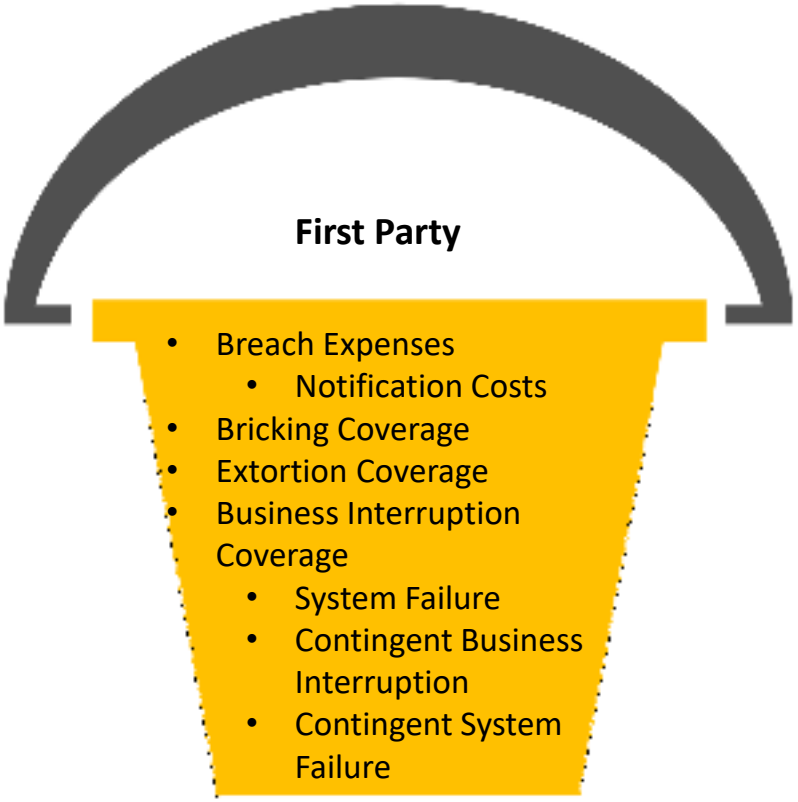
The Combined Ratio Improved 25 Percentage Points in 2022 Amid a 62% Increase in Premiums



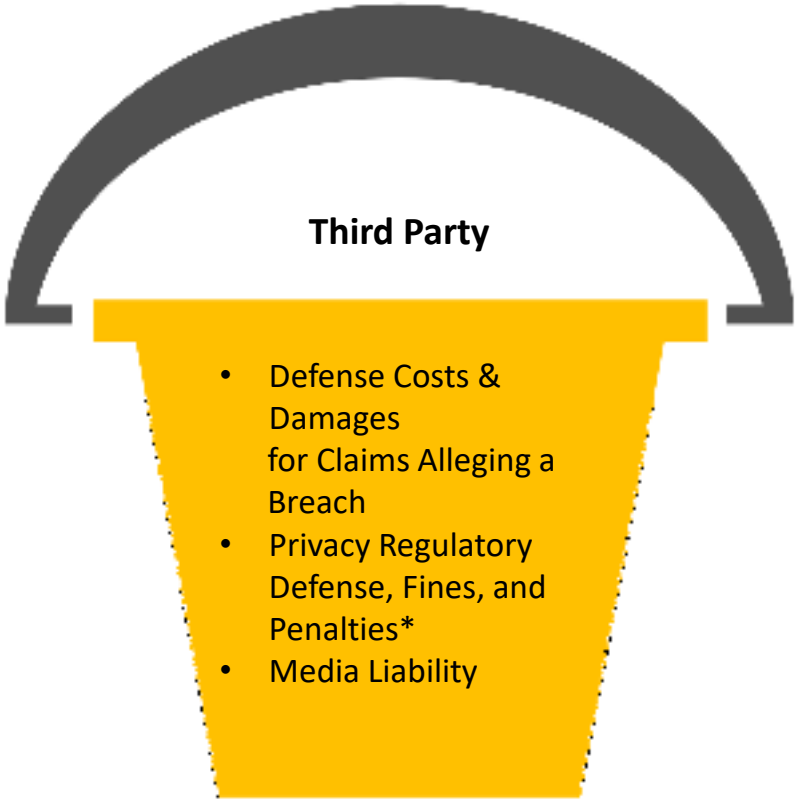
PC Industry Aggregate. LHS - left-hand side axis. RHS - right-hand side axis. DCC - Defense and Cost Containment incurred. DWP - Direct written premium. Note: Statutory Cybersecurity and Identity Theft Insurance Coverage Supplement Data.
Source: Fitch Ratings, S&P Global Market Intelligence

FitchRatings

First/Third Party

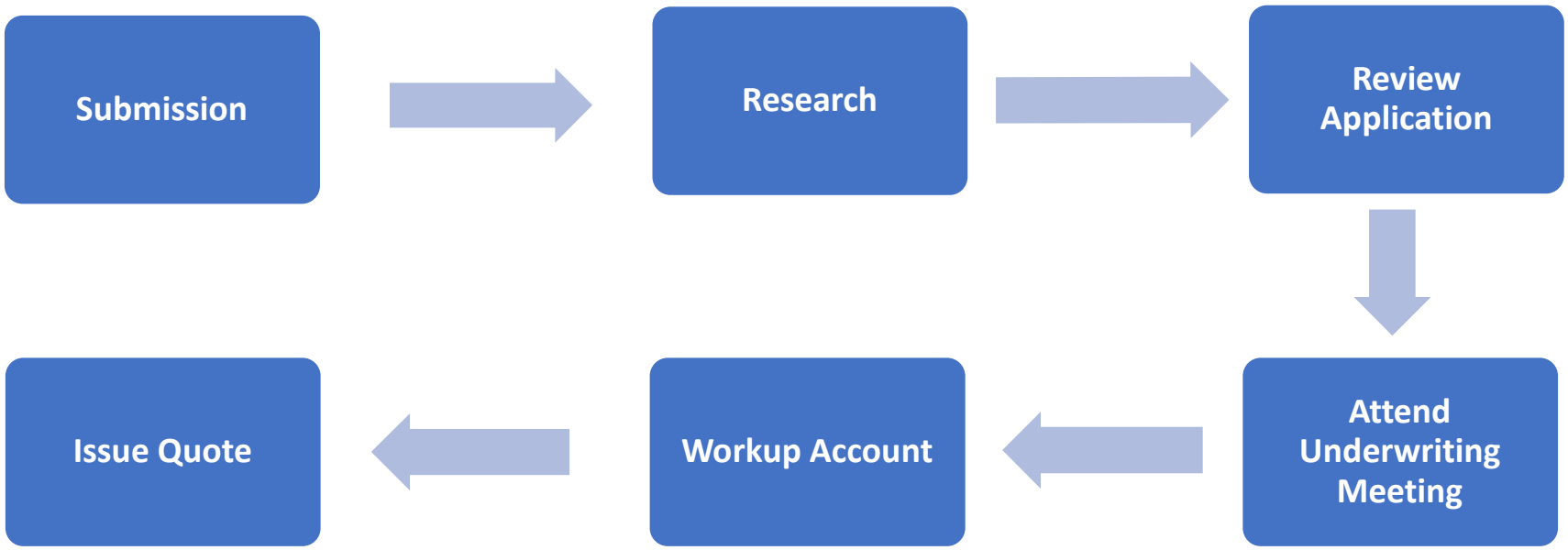


First Party Coverages



Third Party Coverages

General Underwriter Workflow



Submission

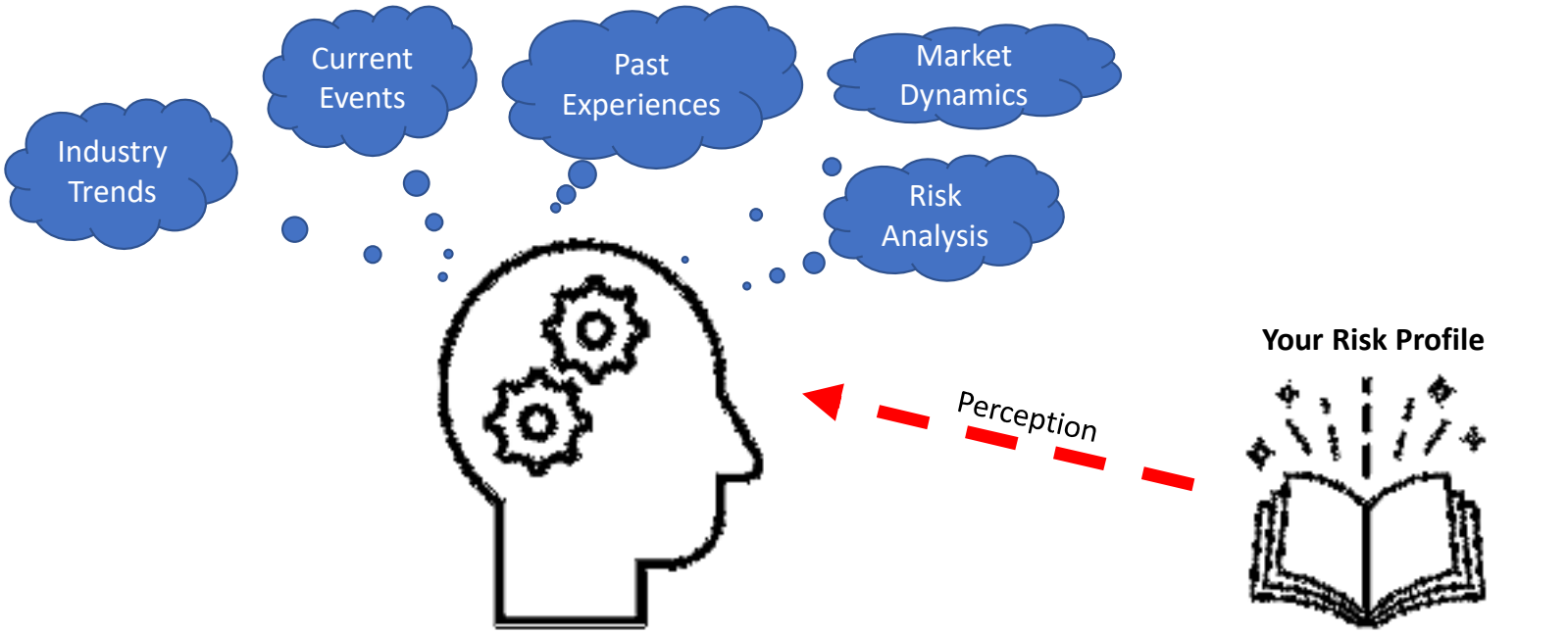
General Cyber Application

Supplemental Applications

- Ransomware Supplemental
- Operational Technology Supplemental
- Privacy Supplemental

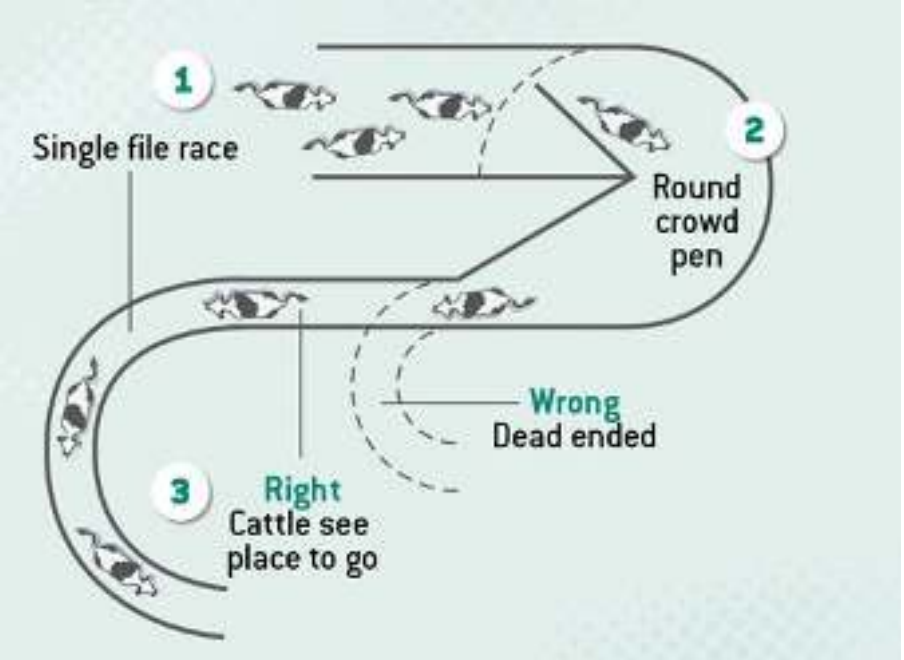
Loss Runs

Mind of an Underwriter



Affordances

- Let compensating controls be known
- Proactively show how your organization has responded to zero-day events (past & present)
- If you have loss history, make it known that you have taken steps to ensure the loss won't happen again
- Provide context wherever you think is fitting
- If you don't have a specific control in place, but you have a project to implement said control, let it be known



Research

- Company Website
- 10-K/Annual Report
- Ongoing litigation
- News of Breach
- Recent Acquisitions/Divestitures

Identifying Business Topology

- How does the business generate revenue?
  - How resilient is the business model against network downtime?
  - How many different units does the business have?
  - Revenue generated from various business units
- Is the business in the process of an acquisition or divestiture?
- Does the business have manufacturing sites?
  - How many?
  - How much of the manufacturing is contracted to 3rd parties?

Application Review

Network Security & Topology

Level 1 – Controls

EDR, MFA, PAM tool, Patching, Segmentation, Backup procedures, etc.

Level 2 – Implementation

% of rollout for EDR, MFA, PAM

How often is the environment scanned for vulnerabilities

Patching Cadence

How often are firewall rules reviewed?

Level 3 – Network Topology

Does the insured have an OT environment?

Segmentation by business unit?

How many domains?

How much of the insured's environment is in the cloud?

Production Environment?

Attend Underwriting Meeting

FILL IN ANY QUESTIONS THAT AROSE FROM THE REVIEW OF THE APPLICATION

ASK SITUATIONAL AND OPEN-ENDED QUESTIONS TO GET A GAUGE OF THE COMPANY CULTURE SURROUNDING CYBERSECURITY

GENERALLY, GOVERNANCE IS COVERED IN THE UNDERWRITING MEETING

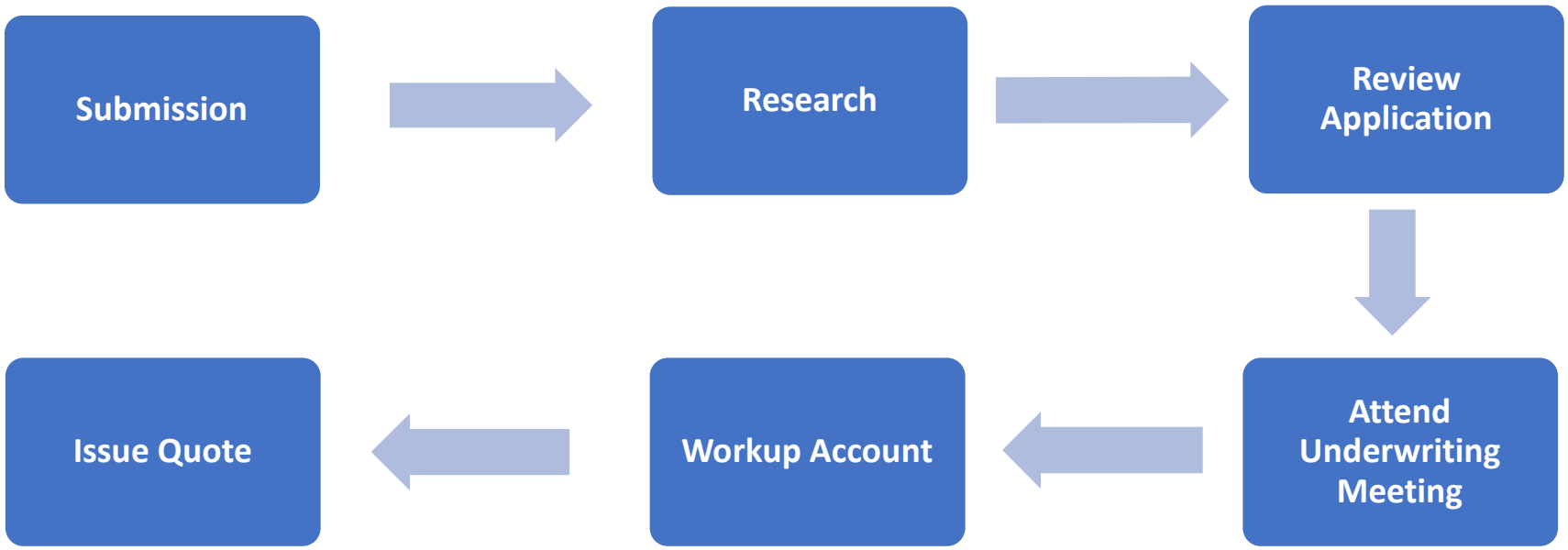
Workup Account

Following the underwriting call, the Underwriter should have all the information necessary to make a judgement on the account

At this stage, the underwriter consolidates all the information they've gathered throughout the process into a single document—called a Workup—that will be presented for approval

In this stage an Underwriter will use a rater (pricing tool built by actuaries) to assist with pricing and they will also use cyber modeling software to assist with risk analysis

General Underwriter Workflow



Submission

- Insured: ApplianceCo
- Revenue: $5B – in the appetite
- Initial Assessment of Controls: Have all the baseline tooling we like to see except for a PAM tool
- Industry: Manufacturing – in the appetite
- Coverage requested: Cyber
- Loss History: Limit loss claim that arose from a business email compromise in 2020

Submission Cont.

- In the body of the submission email the Broker includes an additional message that states the 2020 business email compromise loss originated from a part of the business that ApplianceCo has since divested. The Broker also stated that ApplianceCo has now implemented SPF, DKIM, and DMARC and DLP for email

Research

While looking into the company website we discover that ApplianceCo produces smart appliances

ApplianceCo's 10-K states they have manufacturing facilities in India, Ohio, and Mexico. ApplianceCo also has a contract manufacturer in China that accounts for a 'material' portion of their total revenue

We also discover that ApplianceCo has a financing business that caters to individuals financing their ApplianceCo purchases. This business segment accounts for 30% of ApplianceCo's total revenue

Initial Information Needed following research

- Details about ApplianceCo's software development lifecycle
- How is accesses to the production environment managed?
- Is the financing business segmented from the manufacturing business?
- Are the factories segmented?
- Is IT segmented from OT
- Are any of ApplianceCo's products produced at a single factory?
  - How much stockpile does ApplianceCo store in the event of downtime?

Application Review

Level 1 - Controls

- An addendum attached to the application states that although there is no pam tool, privileged accounts require a 25-character password and are rotated on a quarterly basis. There is an ongoing project to implement a check in/out solution within 6 months
- Firewalls are in place
- EDR is in place

Level 2 - Implementation

- MFA is required for all remote access to the network
  - Can not access SaaS applications without company owned device and token
- EDR is configured to block
- All employees have local admin privileges
- Disaster recovery of critical systems is tested once every two years
- Firewall rules are reviewed quarterly

Level 3 – Network Topology

- Business units are segmented via firewall
- IT is segmented from OT

General Info

- 15 domain admins

Information Needed Post Application Review

Questions for Underwriting Meeting

- Details regarding ApplianceCo's software development lifecycle
- How is accesses to the production environment managed?
- ~~Is the financing business segmented from the manufacturing business?~~
- ~~Are the factories segmented?~~
- ~~Is IT segmented from OT~~
- Are any of ApplianceCo's products produced at a single factory?
  - How much stockpile does ApplianceCo store in the event of downtime?
- I noticed 15 domain admins – is this across multiple domains?
- Is a just-in-time tool used to manage local admin access?
- Are there any plans to increase the cadence of DR testing for critical systems?

Workup

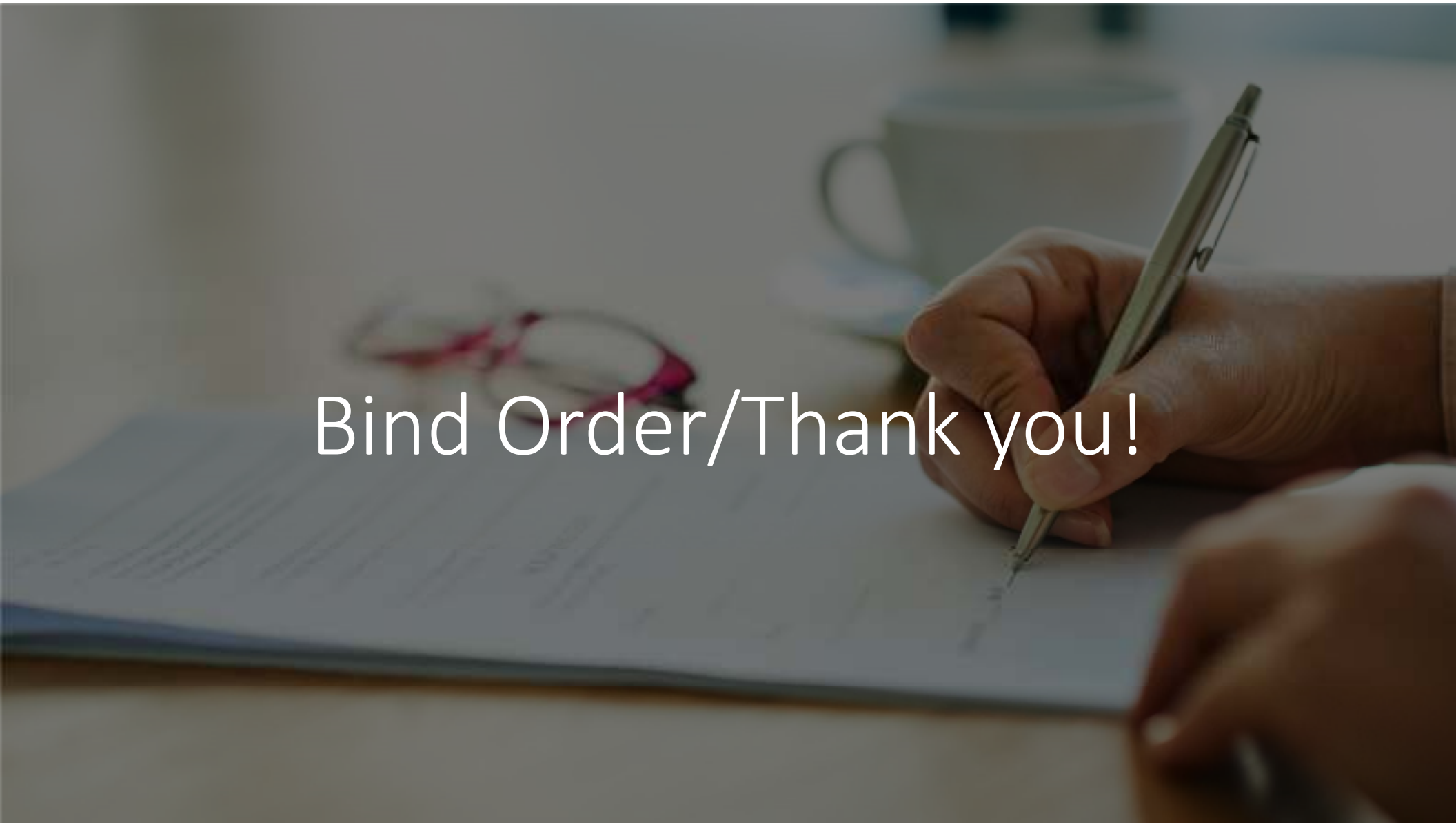
- Underwriting Summary
  - Overall good controls
  - Need to work on frequency of disaster recovery
  - Although local admin privileges are administered through just-in-time solution, I would prefer a stricter culture around local admin rights
  - Good segmentation practices
  - Large portion of the business is less susceptible to business interruption loss
- Rated Pricing: _____
- Modeled view of the risk:_____
- Underwriter recommended price:____

Takeaway: Cyber risk is not statistically well understood. Given the relatively new and evolving nature of cyber risk, there will likely be a material delta between rated pricing, pricing from 3rd party modelers, and underwriter recommendations.

Issue Quote

Quote issuance can be an iterative process depending on the account

Once initial terms are released, subsequent adjustments can be made to pricing and coverage specifics based on negotiations between the Underwriter and Broker


Bind Order/Thank you!