Crown Jewel® Protector

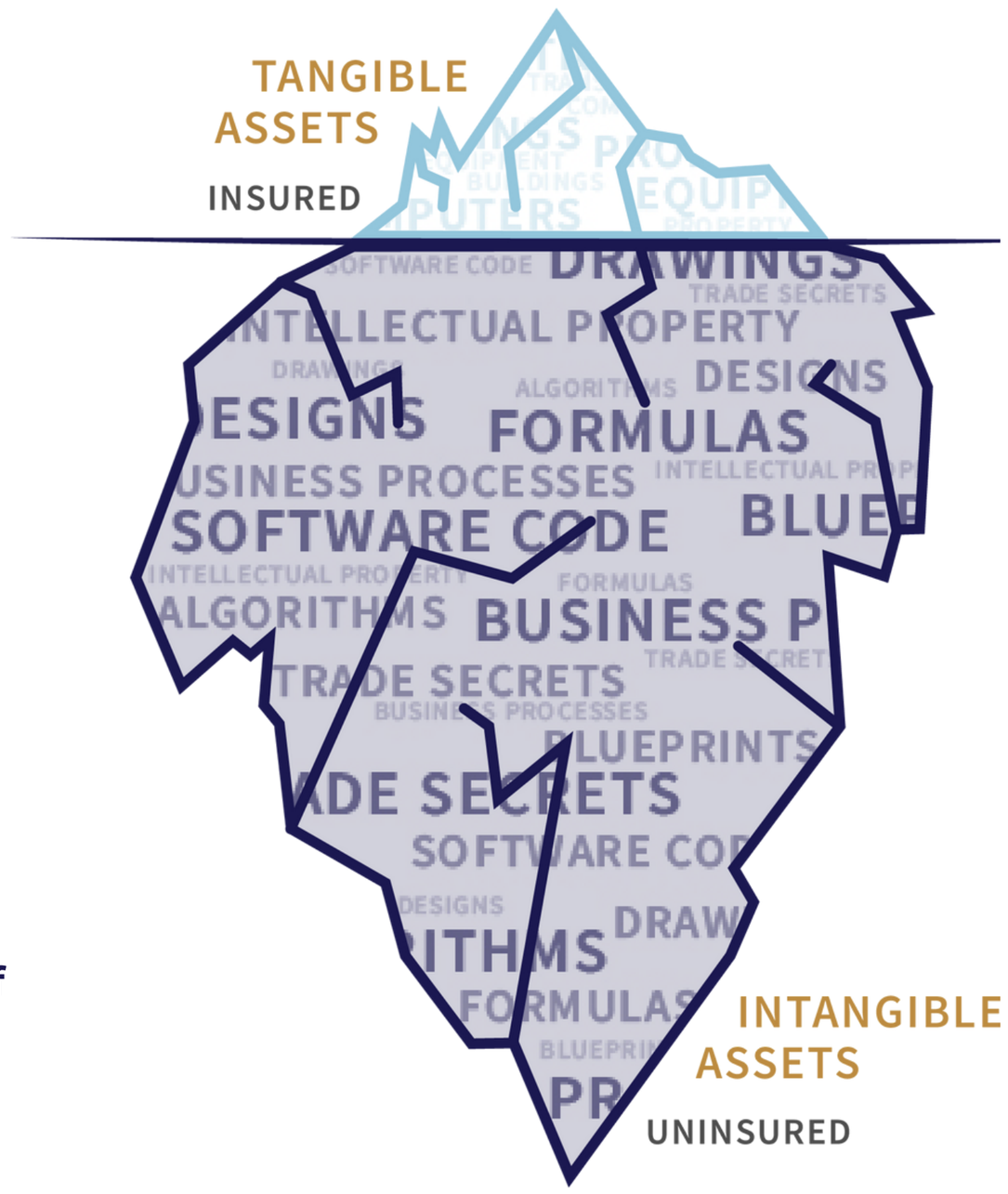
According to Ocean Tomo as of 2022, 90% of the S&P 500 value (estimated at $38 Trillion) is said to be intangible/intellectual property assets. Trade secrets are the fastest growing and most critical intellectual property asset category, yet there has been inadequate emphasis on identifying, managing, and protecting those assets in a meaningful way. Crown Jewel® Insurance has developed a formal Trade Secret Asset Risk Management (TSARM) process, including a ground-breaking first-party insurance coverage- a game-changer in the insurance industry!

- **Pre and Post Loss TSARM:**
  - **Identification and tracking via blockchain**
    - **Blockchain creates a perfect record, available instantaneously, used to support the grant of a TRO or ex parte seizure, and also used in litigation if necessary. Currently, many cases get dismissed pretrial due to lack of proper documentation/evidence, which this software cures.**
    - **The Discovery process is drastically shortened and the insured can save 50% or more in litigation expenses by using this system properly.**
  - **Security & enforcement assessment/recommendations**
  - **Fair Market Valuation**
  - **Dark Web Monitoring**
  - **Claims management, IP enforcement and litigation services**
    - **In cases where one or more experts were used, the average damages were approximately $24 million versus only $4 million when no expert was used.**

- **Key Benefits:**
  - **Insurance coverage provides critical financial protection in the event of misappropriation of a company's most valuable assets.**
  - **Allows Trade Secrets to be MONETIZED:**
    - **Increasing the overall value of the company.**
    - **Allowing for lenders and investors to deploy capital using these assets and/or insurance proceeds as collateral (During M&A Transactions or stand alone).**
  - **The TSARM process alone will make the vast majority of corporations much better prepared to protect and defend against the threat of misappropriation.**
  - **Provides visibility to company Boards, Executive Leadership and investors.**

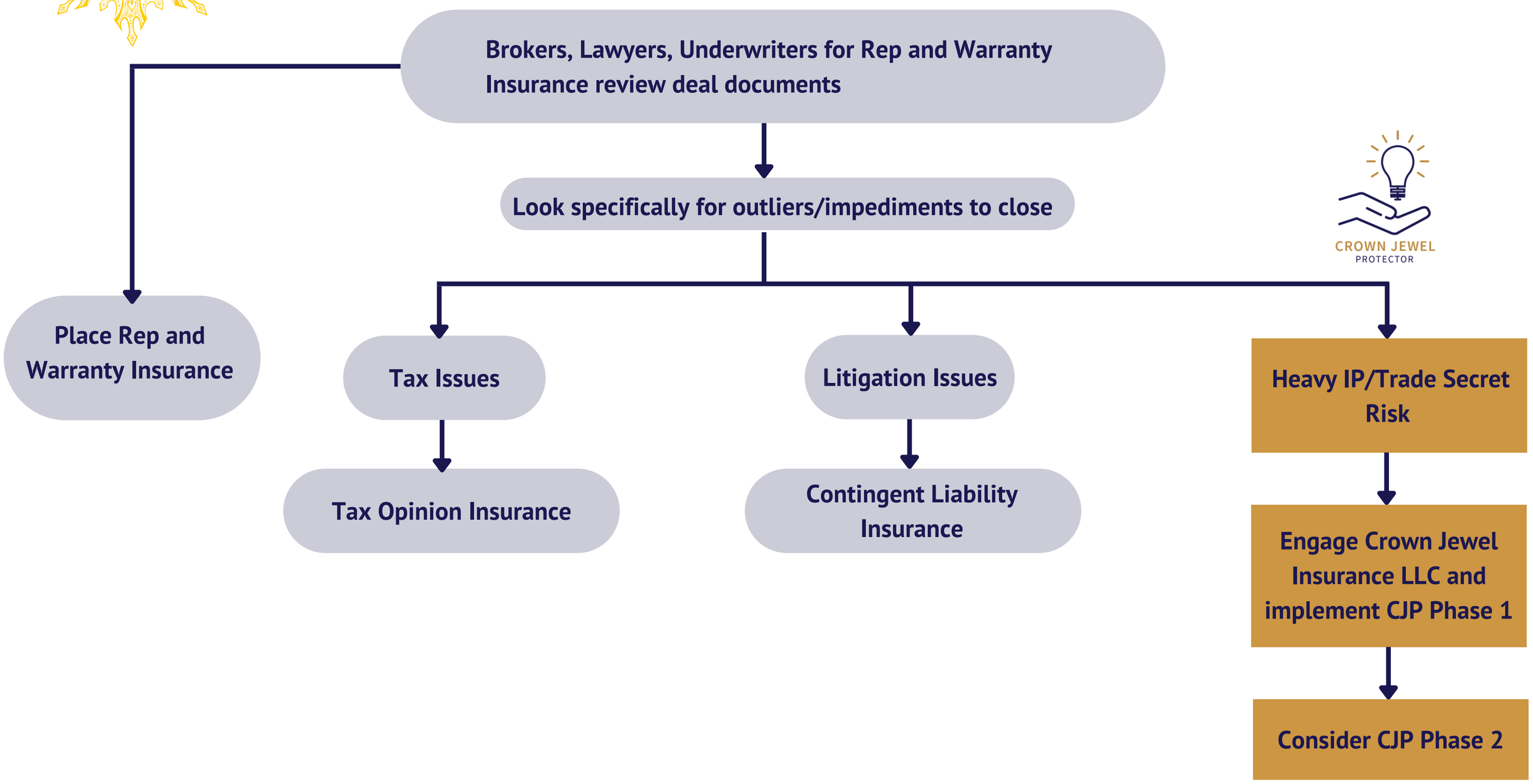
What is a Trade Secret?
All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, that

- **The owner thereof has taken reasonable measures to keep such information secret –and–**
- **The information derives independent economic value, actual or potential, from not being generally known, and not being readily ascertainable through proper means.**



Where does TSARM fit in the context of M&A Transactions?

M&A Due Diligence Process (simplified)



Buyer Beware: A Case Study on What a Rep & Warranty Policy Won't Cover

Intellectual Property theft is at the core of a claims issue that is not likely to be covered under a typical Rep and Warranty policy or any other insurance.

The following real-life claims scenario is illustrative of this point:

A. Buyer is purchasing a company largely for its IP, some patents but mostly Trade Secret Assets (TSAs). The deal is approximately $10M (could be much bigger obviously)

B. The Buyer purchases a typical R&W policy, which triggers off of a Breach (of Rep or Warranty). *Unrelated aside; this is very confusing because in Cyber we speak about Breach as a trigger for coverage all the time too; but it's a "security breach" or "privacy breach"

C. In the transaction documents, the Seller represents, as typical, that they (paraphrasing):

1. own the IP they are bringing to the table,

2. as far as the Specified Persons (CEO, CFO, GC) are concerned, they do not have Actual Knowledge of any theft or misappropriation of any IP. The deal document then goes much further and says Seller does not know of any third-party custodians of those TSAs (who have been granted legal access) that may have disclosed or otherwise hindered or negated their value, AND they also do not know of anything that would prevent the recovery of those assets, and

3. are using:

i. "industry standards" and regulatory requirements to protect their data generally (they have a SAS 70 II and do Penetration testing every year, fix all known security vulnerabilities…(this is a standard no one should actually agree to; it is not possible), and

ii. "Reasonable efforts" to protect Trade Secret Assets (TSAs).

D. The deal goes through, and months later (as is very typical in a cyber event), they discover that the Seller had a "security breach" involving the theft of a lot of data, including both PII (a "privacy breach") and what they believed to be TSAs.

E. The Buyer now sees the deal as far less valuable because the IP (the main reason they bought the company) has been compromised. Buyer wants to collect under the R&W policy.

F. The R&W market DENIED the claim because there was no Breach of an R or W – the Seller did have "standard" procedures in place, but the theft happened anyway.

G. To make matters worse, the Seller was not able to demonstrate that they were making "reasonable efforts" to protect the R&D they considered TSAs; therefore, they could not get a TRO or seek damages for the TSAs. Most companies do not keep adequate evidence of their trade secret protection because they don't even determine up front what and where their trade secrets are, much less what they are worth.

To placate the client, the carrier is going to pay a small fraction of the claim. The Buyer is now left with a company that is not worth the value they paid for it.

If the Buyer did continue the Sellers' cyber insurance policy which had, say, a $2M limit, it may respond to the "breach response" and other costs associated with the PII, but it will NOT cover the value of the TSAs. Cyber Insurance never covers speculative value or future income of any asset.

Incidentally, an argument could be made that there is a breach of the Rep because the Seller did not have a mechanism in place to detect theft of IP assets and/or a process in place to recover them or seek Damages on the back end.

In summary, these types of losses may happen on a regular basis, as the average time to discover a cyber breach is an estimated +/-225 days (Note: the trade secrets could have been stolen by a former employee and the same lag time may occur). Perhaps more important than the fact that the R&W policy won't pay is the fact that their IP is impaired now and no longer has any value as a Trade Secret.

The TSARM process, with the Crown Jewel® Trade Secret Insurance policy at the center of it, would have mitigated or even prevented this entire situation. Blockchain evidence of what the TSAs are and how they are protected (metadata only) plus dark web monitoring and an up-front security assessment specifically looking for "chatter" about the Sellers' trade secrets, etc. would have given ample evidence of "reasonable efforts" and would have allowed for much quicker knowledge of the security breach. Therefore, may have led to an ex parte seizure or at least Damages on the back end. In the meantime, the insurance would have paid the Buyer the Fair Market Value of the scheduled TSAs.

This has big implications for IP heavy M&A deals. In the above scenario, the Buyer should want to have Crown Jewel Protector in place on a continuous basis because the hack could have easily both occurred and been discovered post-close. This process is equally applicable OUTSIDE of the Transaction environment for any company that has a heavy IP portfolio.

Trade Secret Risk Management Audit (Phase 1)

Step 1: Identification

Cataloging of potential Trade Secret Assets and "Defendability Score" via blockchain

Step 2: Valuation

Third-Party Expert Valuation to determine Fair Market Value of Trade Secret Assets

Step 3: Preliminary Legal Review

Document Assessment: Employment Contracts, NDAs, Third-Party Service Provider/Customer Agreements, etc.

Trade Secret Asset Risk Management (TSARM) Confirmed

Ready for CJP Phase 2

Benefits of Completing Trade Secret Management Audit Phase 1

- Trade Secrets identified and documentation ready to use as evidence if misappropriation occurs
- Expert valuation of IP assets immediately increases company value
- Provides transparency and protection to Senior Leadership and the Board e.g. oversight responsibilities
- Increases confidence of potential buyers around security and viability of IP assets

Next Up Phase 2: Risk Mitigation and Litigation Readiness

- Security Scan/ Dark Web Monitoring
- Threat Assessment
- Negotiation and placement of Crown Jewel® Trade Secret Insurance
- Post Breach
  - Forensics/Investigation
  - Asset Recovery
  - Litigation for damages as required
- All post-breach expenses are paid for as part of the insurance premium