AUGUST 2024

BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

SUCCESSFULLY CONFRONTING STRATEGIC RISK:
THRIVE OR SURVIVE

“Bad actors targeting US Corporate Trade Secrets: the SEC’s Call to Action”

Nation-state malicious actors have sharpened their focus on the Intellectual Property (IP) of US corporations, with Critical Infrastructure companies, in particular, in the crosshairs of these relentless campaigns. The transparency of the patent system lays bare the details of our ingenuity for easy targeting the moment patents are granted. Trade secrets, the lifeblood of our competitive advantage, are inherently more resilient to exploitation—but this resilience is only as strong as the protective measures deployed to keep them secret. Moreover, the modern workplace, with work-from-anywhere access and BYO anything, has made it easier to accomplish the unauthorized transfer of sensitive information. Knowledgeable insiders and an increasingly porous cyber environment put at risk the know-how that drives market leadership. The evolving threat landscape demands a recalibrated and robust approach to safeguarding our corporate “crown jewels”.

Intangible assets have surged in value, now comprising an estimated 90% of the S&P 500's value (reported by Ocean Tomo in January 2021). Intellectual Property (IP) is the cornerstone of this intangible asset valuation, with trade secrets holding the lion’s share. These assets, often uninsured, are believed to represent a staggering value exceeding $10 trillion). This figure does not account for the value of ideas and innovation fueling small and medium businesses, private entities, or government and military sectors.

Mary Guzman

Founder and CEO,
Crown Jewel Insurance

Leading Crown Jewel® Insurance, I champion innovative approaches to protect intellectual property, leveraging a deep understanding of cyber insurance and financial risk management honed over decades in the industry. Our team, through the Crown Jewel℠ Protector program, has pioneered trade secret insurance, a first in the industry backed by Lloyd’s of London, underscoring our commitment to safeguarding companies' most valuable assets.

The recognition as a 2021 Business Insurance Woman to Watch and the 2023 Innovation Award Winner reflects our collective successes. We specialize in crafting unique risk management strategies that address the evolving landscape of IP risks, with a focus on trade secrets, and working in collaboration with valuation and damages experts, law firms, and cyber security experts to fortify our clients' defenses against IP theft.

I am a frequent speaker and author regarding the ever-increasing exposure of theft of trade secrets via cyber and other means and work through various professional organizations to promote awareness of this problem. I am fortunate to be on the trade secret committee of the AIPLA and Chair the trade secret committee of the USIPA.

AUGUST 2024

BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

The critical trade secrets of a company are the foundation of its competitive advantage: the promising assets in the R&D pipeline, the algorithms, formulas, designs and manufacturing processes that make a firm better and faster than its competition. Trade secrets value is inextricably linked to their concealment; disclosure doesn't merely diminish their value—it annihilates it as a protectable trade secret, ending a firm's exclusive rights to leverage that asset. This loss of return on investment is not theoretical; it is a real void where once there was value.

So much intellectual property is at risk because of a stark lack of oversight in corporate risk management. This is due to an incomplete understanding of the value of these assets and how to protect them. Many organizations also believe that existing insurance policies cover the theft of trade secrets: they do not. This gap leaves these assets completely vulnerable if compromised. Leadership and Boards that fail to address the risk of misappropriation—or neglect to make the necessary disclosures—are exposed to compliance and shareholder risk. It is a clarion call for Boards to navigate increasingly treacherous waters with foresight and to fortify their company's defenses against the theft of their most prized assets.

CHALLENGING ENVIRONMENT LEADS TO SHIFTING STRATEGIES AND GREATER RISK.

Today, the U.S. patent system is navigating turbulent waters. An astonishing 75% of patents are being overturned upon review by the Patent Trial and Appeals Board, nullifying the time, effort, and money spent to secure the patent in the first place. A vast array of assets fall outside the patentable realm, most notably the use of Artificial Intelligence. Thus far, the Patent Office and courts have disallowed patents for outputs of Generative AI, citing that they are not created by a "human."

Unlike the other types of IP, trade secrets are a "litigation right," meaning the only way to know for certain if you have one is to litigate. Therefore, failing to identify these assets and put requisite "reasonable measures" around them negates a company's ability to maintain its integrity as a trade secret. And, this potentially prohibits compliance with regulatory mandates such as the SEC Cyber Disclosure Rule. Moreover, the potential shift in the legal landscape regarding non-compete agreements by the FTC necessitates a strategic realignment of protection mechanisms.

JULY 2024

BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

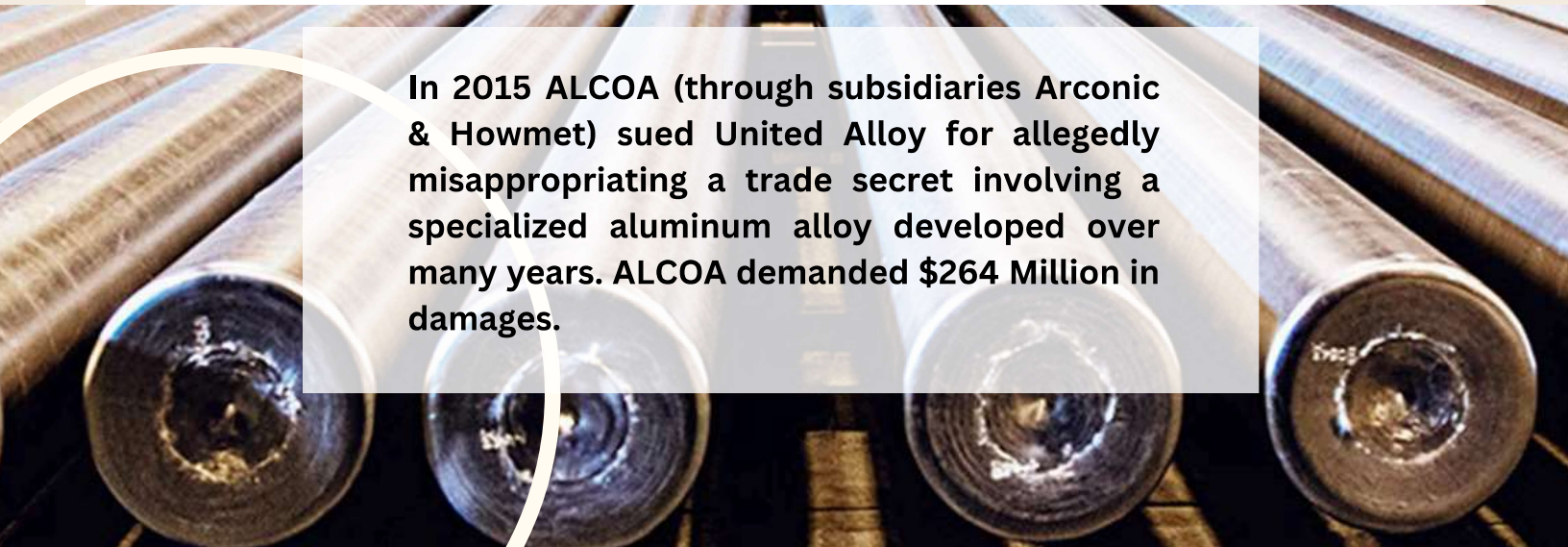
The Pending Ban on Non-Compete Agreements

The Federal Trade Commission's ban on these agreements was originally slated for a September 2024 effective date, although the actual date will be subject to the outcomes of current legal proceedings. For years, non-compete agreements have been the bulwark against the risk of employees transferring sensitive competitive information, clientele, or fellow employees to rival firms. They have served as a critical line of defense in protecting trade secrets, especially in scenarios where alternative strategies were not in place. Despite this, it's crucial to recognize that protecting trade secrets from employees or former employees is not solely dependent on these agreements. In fact, tort law prohibits the misappropriation of trade secrets from former employers, with the potential for severe legal repercussions up to and including criminal prosecution, hefty fines, and imprisonment for the offending individuals.

Moreover, the landscape at the state level underscores a definitive move away from non-compete agreements regardless of the outcome of the federal ban. Four states have completely prohibited non-compete agreements, and thirty-three states partially ban them. The outcome of the Presidential election will also impact this issue.

The demise of the noncompete underscores the necessity for a comprehensive approach to confidentiality in employment, contractor, and third-party agreements. The emphasis must now be crafting contracts with precise language that unequivocally protects sensitive corporate information and trade secrets. The specificity and enforceability of these confidentiality clauses will become increasingly critical in safeguarding a company's intellectual assets in an era where non-compete agreements may no longer be viable.

ALCOA, Inc. v. United Alloy - A Classic Case



In 2015 ALCOA (through subsidiaries Arconic & Howmet) sued United Alloy for allegedly misappropriating a trade secret involving a specialized aluminum alloy developed over many years. ALCOA demanded $264 Million in damages.

Figure 1

The Alcoa case is a classic example of a corporation that lost its key innovation because it was unable to demonstrate that it had a defendable trade secret in the first place. Had ALCOA enjoyed the benefits of a trade secret-focused risk management program, the outcome of the trial would have likely been very different.

The fact that ALCOA could not document evidence proving that the invention was not known in the industry at the time of the innovation and alleged theft (eight years prior) killed the case. It is very difficult for a non-technical jury to discern this nuance so many years after the fact, with expert witnesses on both sides. This is a key reason why immutable evidence, such as a "registry" of trade secrets stored on blockchain, is critical evidence of the existence of a trade secret.

Embedded Knowledge:
Unlike patents, trade secrets are often created in another part of the organization, derived from years of strategic development and operational refinement.

KEY FACTORS TO ASSESS TRADE SECRET RISK

Trade Secrets Precede Patents:
Inventions are confidential until patent publication, making trade secrets the only way to protect innovation during R&D.

High R&D Investment:
Companies with R&D spending over 10% of revenue or 5% for a single innovation face significant trade secret misappropriation risk.

Value of Negative Know-How:
Lessons learned from failures (or smaller iterative improvements), known as "negative know-how," often create some of the most valuable trade secrets.

Questions for the Leadership Team:

Has your company identified innovation assets that, if stolen, could be “material” to future earnings?

Does your organization keep an inventory (registry) of projects or innovations that may qualify as trade secrets?

Who in your organization is the gatekeeper for these competitive assets?

Are trade secret assets treated with additional security controls above and beyond those used to protect other important corporate assets?

BUILD AN EFFECTIVE TRADE SECRET ASSET RISK MANAGEMENT (TSARM) PROGRAM TO PROTECT TRADE SECRETS

Organizations should establish a Trade Secret Asset Risk Management (TSARM) program led by a cross-functional team. A TSARM framework should be designed to unearth hidden value, prevent theft of a company’s competitive value, and formalize a process to ensure a successful and quick recovery (“litigation ready”). Key components of the framework are illustrated in Figure 2.

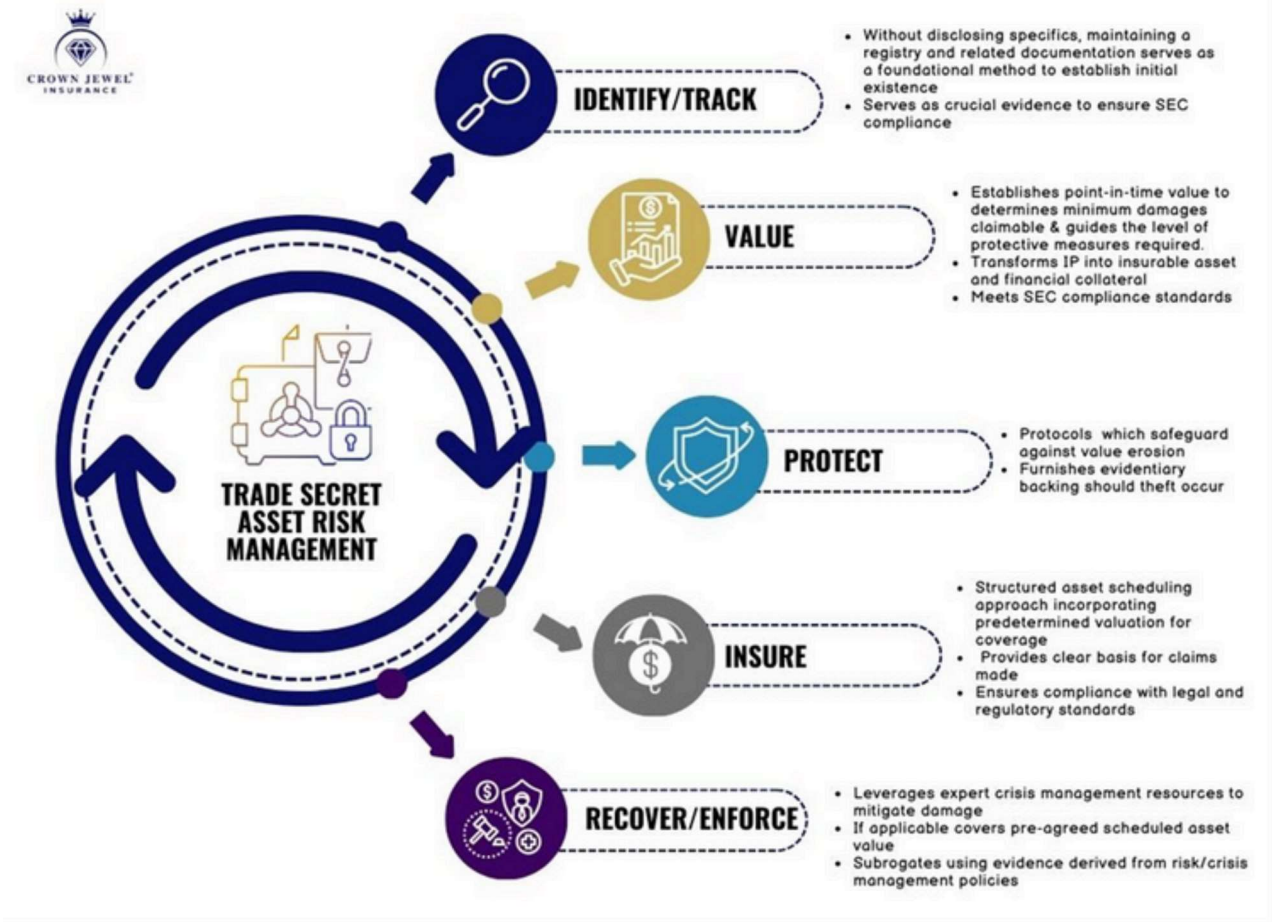


Figure 2

The five key steps in a Trade Secret Asset Risk Management Protection Framework process will be quite familiar to those involved in ERM strategies; they simply address an asset class and a set of legal issues unfamiliar to most. The approach provides the input required to comply with the SEC Cyber Disclosure Rule and fill gaps left by the FTC ban on non-competes.

The EONA Proofs

A critical component of any trade secret risk management program is the asset-specific ability to demonstrate the “EONA Proofs.”

EONA stands for "Existence, Ownership, Notice, and Access:

Existence of a trade secret – THE fundamental starting point to any enforcement action (many jurisdictions will not even allow Discovery to begin if you cannot demonstrate, with specificity, what the trade secret is). A company must provide evidence that the asset:

a) was developed independently
b) is not known in the industry
c) is sufficiently valuable to the company or its competitors, and
d) “reasonable measures” are being used to maintain its secrecy.

Trade secret claims are often decided on any one of these factors alone.

Ownership – the company actually owns the rights to the asset (as opposed to the inventor)

Notice – the people who have access to the know-how are explicitly told that it is a trade secret (or at least valuable confidential information).

Access- the misappropriating party had access to the asset (even if through a third party).

For Boards, the convergence of fiduciary responsibility with the escalating threats underscores the urgency of crystallizing risk management policies. But there is a path forward: a phased-in cross-functional approach to trade secret protection.

Questions for the Leadership Team:

1 - If your company has a Trade Secret Asset Risk Management program, is it part of your enterprise risk management program?

2 - Has your company documented how to make a materiality decision factoring in consequential losses beyond immediate monetary impact?

3 - Has your organization decided how it will determine when a crown jewel has been stolen?

4 - How are trade secrets managed when third parties require access as a function of their outsourcing duties?

AUGUST 2024

BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

The SEC CyberSecurity Disclosure Rule and Trade Secrets

The SEC's Cybersecurity Disclosure Rule came into force in December 2023. This rule mandates a detailed discussion of corporations' processes for assessing, identifying, and managing material risks from cybersecurity threats.

Key Highlights of the SEC's Cybersecurity Disclosure Rule:

Mandatory Disclosures: Corporations must provide detailed discussions on processes for assessing, identifying, and managing material cybersecurity risks, elevating visibility in 10-K reports.

Repositioning Disclosures: Cybersecurity disclosures are moved from the Risk Factors section to a more prominent position, ensuring heightened investor awareness.

Material Risk Definition: While "material" risks are not explicitly defined, the SEC emphasizes competitive advantage and reputation, positioning high-value trade secrets under this requirement.

Broad Incident Reporting: Companies must disclose the "nature, scope, and timing" of cybersecurity incidents that may materially affect operations or finances, including events occurring before the rule's enactment.

Urgency in Reporting: If an incident is deemed material, companies must file an 8-K with the SEC and shareholders within four business days, highlighting the critical nature of these disclosures.

Guidance on Materiality: Companies can utilize established Cyber Security Frameworks, such as NIST, to assess materiality, considering assets material if they constitute at least 0.5% of total asset value or 5% of revenue.

For Boards, this raises a central question:

How will your organization know which assets meet a materiality threshold if they have not been identified and valued?

22 companies filed 35 reports on cybersecurity incidents since the rule became effective on December 18, 2023. These filings, a mix of new disclosures and updates to existing filings as further details emerge, have so far focused solely on the qualitative fallout of these incidents. Notably, none have delved into the quantitative repercussions—such as potential revenue loss or the cost of remediation. High-profile breaches, such as the hacking of executive emails at Microsoft, Hewlett Packard, and United Health, raise critical questions about the content exposed and its significance to corporate competitiveness. In mid-July, Disney announced that the company's Slack internal communications platform was compromised in a 1.1TiB hack; the breach revealed information on future projects and stood as a solitary acknowledgment of the potential competitive harm from such breaches. How the SEC and shareholders react will evolve, likely becoming harsher as plaintiffs' attorneys raise concerns for all. One recent trend is that hackers are starting to act as whistleblowers by alerting the SEC if they have successfully hacked and stolen potentially material assets when but see that no disclosure has been made.

Trade secret insurance could become a game changer for many companies. Trade secret due diligence processes help to pinpoint and document invaluable trade secrets, establish a value, and affirm that sufficient protections are in place. When a crisis hits an organization, a trade secret insurance policy will cover the costs for legal and forensic experts. Armed with underwriting due diligence and forensic data, these experts would be a front line in securing injunctive relief to protect assets. Successful court outcomes mean that trade secrets remain a competitive advantage. Also, in the event that initial enforcement efforts did not cure the impairment, insurance coverage would compensate the company for the value of the lost asset up to the policy's limit.

Beyond immediate crisis management, insuring trade secrets can monetize them overnight, making the company more attractive to lenders and investors and boosting its valuation.

Questions for the Leadership team:

- Does your CFO or finance team assign financial value to trade secrets (including development costs)?
- Is your company currently addressing the potential quantum of this risk and how it is mitigated in your 10-Ks?
- Has your company reviewed its Cyber, Crime, and D&O policies to see where there are gaps in coverage for IP-related losses or the value of the assets themselves?
- Has the company considered purchasing trade secret insurance, which is similar to a crime policy, covering the value of these assets against theft?

Conclusion

It is essential for companies to maintain a robust trade secret risk management framework. This framework should mimic established ERM policies and procedures and be supplemented by focusing on the EONA proofs. Since trade secrets are fragile “litigation rights”, it is crucial to document and create immutable evidence of the Existence, Ownership, Notice, and Access of each critical asset, prioritizing the most current and future value to the company. This program can be reinforced by robust insurance coverage designed to fill gaps in existing policies. Although the market for this product is nascent, demand will drive supply as it always does.

Cited Sources:

https://oceantomo.com/intangible-asset-market-value-study/

https://www.reuters.com/legal/legalindustry/increasing-importance-trade-secret-protections-us-businesses-2024-04-02/

https://www.law.com/corpcounsel/2023/08/07/ruling-against-company-that-called-a-lawsuit-without-merit-likely-to-sideline-widely-used-phrase/

https://www.gibsondunn.com/sec-adopts-new-rules-on-cybersecurity-disclosure-for-public-companies/

https://www.forbes.com/sites/bobzukis/2024/03/04/companies-are-already-not-complying-with-the-new-sec-cybersecurity-incident-disclosure-rules/

https://www.crownjewelinsurance.com/blog/trade-secret-litigation-severity-way-up citing August 2021 Reuters article by R. Mark Halligan; EONA Proofs

https://www.reuters.com/legal/litigation/universal-alloy-wins-alcoa-trade-secret-trial-over-airplane-wing-parts-2023-07-26/

BRC
BOARD RISK COMMITTEE

Who We Are

The Board Risk Committee (BRC) is a nonprofit, non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest.

SUSAN C. KEATING
BRC CEO

CATHERINE A. ALLEN
BRC FOUNDER AND CHAIR

CONTACT INFORMATION

Catherine A. Allen, Founder, Chairman, Board Risk Committee
cathy@boardriskcommittee.org

Susan C. Keating, CEO, Board Risk Committee
susan@boardriskcommittee.org