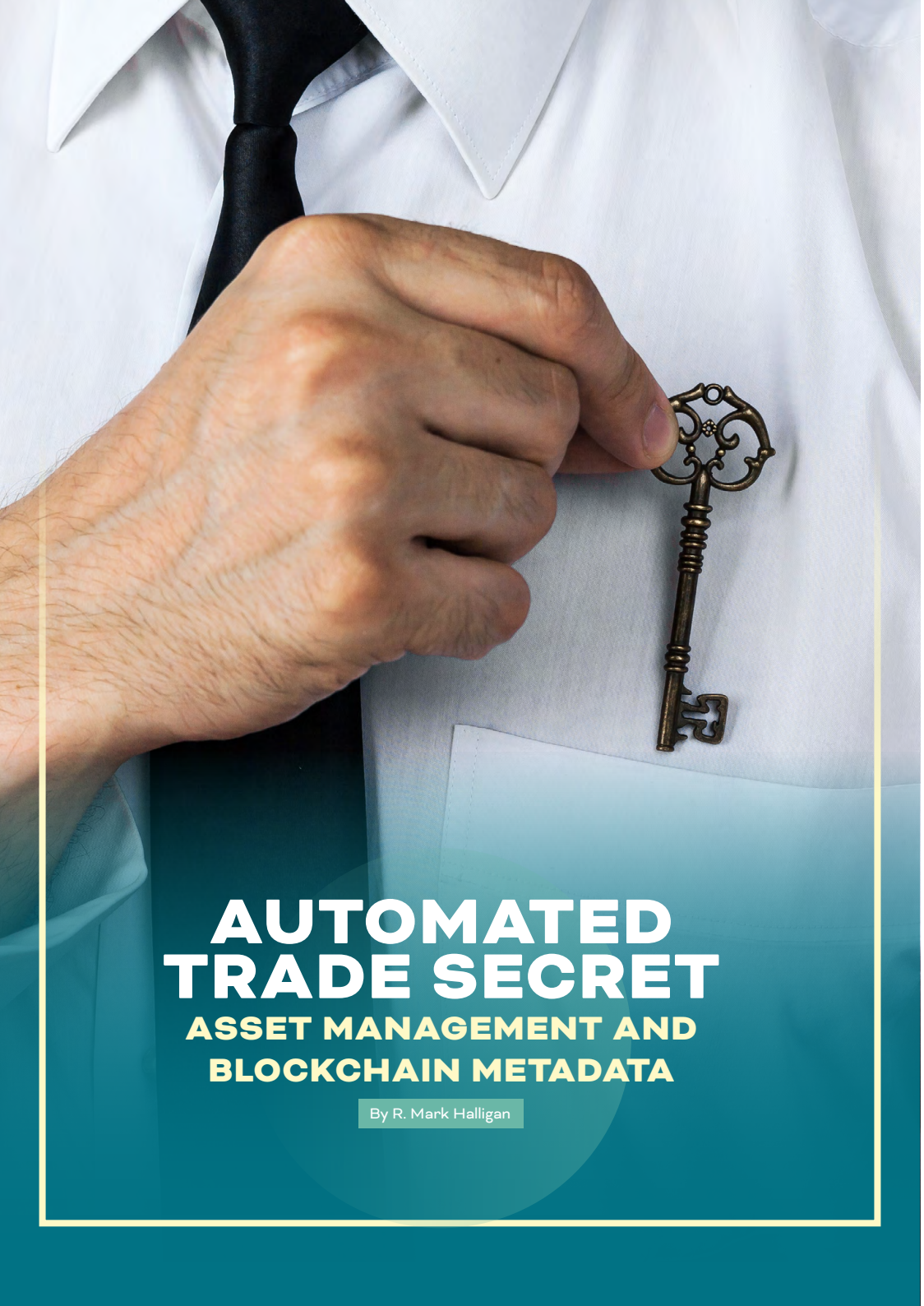
INTELLECTUAL PROPERTY

CorporateLiveWire

EXPERT GUIDE 2022

www.corporatelivewire.com



AUTOMATED TRADE SECRET

ASSET MANAGEMENT AND BLOCKCHAIN METADATA

By R. Mark Halligan

There is another intellectual property revolution on the horizon, and it is called automated trade secret asset management (TSAM). Using computerised TSAM tools to identify, classify, protect and value trade secret assets, will unleash and fuel the exponential growth of intellectual property assets in the 21st century.

Recent studies show that over 80% of senior executives recognise that trade secrets are critical and essential to their businesses. 50% of these senior executives say that trade secrets were more important than their patents and trademarks. Even more (69%) say they foresee trade secret protection becoming more critical than safeguarding other types of intellectual property because of the rapid and furious pace of innovation. Over 60% of these senior executives say that protecting trade secret assets is a board-level issue. Nearly one-third of the respondents ranked the protection of trade secret assets a top-five concern.

There are four stages of trade secret asset management: identification, classification, protection and valuation. The four stages cannot be juggled around. Identification precedes classification; identification and classification precede protection; identification, classification and protection precede valuation.

The problem lies in the starting point for trade secret asset management. Everyone starts at the third stage – protection – with policies, practices, and procedures and a labyrinth of physical, contractual and technical requirements for "protecting" trade secret assets before the identification and classification of specific trade secrets. Without the identification and classification of trade secret assets before security measures are implemented, the protection measures are doomed to fail – you cannot protect "it" if you do not know what "it" is.

A recent study by the Economist Intelligence Unit (EIU) which is the research arm of The Economist Group, publisher of the Economist, illustrates the trade secret conundrum. The EIU surveyed 314 senior corporate executives based in six countries: China, France, Germany, Singapore, the United Kingdom and the United States from six sectors of the economy: consumer goods and retail; finance; energy and natural resources; life sciences; manufacturing and technology; technology, media and telecommunications. The interviews were conducted in January and February 2021.

Top threats to trade secrets were ranked by senior corporate executives: weaknesses in cybersecurity (49%); employee leaks (48%) competitive intelligence (27%); third-party service provider risks (26%); corporate espionage (24%).

The senior executives were then asked which practice would be most effective in preventing potential threats to trade secrets: installing computer safeguarding and cybersecurity software (53%); confidentiality agreements and policies (46%); restricting digital and physical access to documents (42%); introducing a culture with incentives for trade secret protection (31%); avoiding cloud storage of important trade secrets (27%).

These security protocols have been available for years, but these practices put the cart before the horse. This is the current trade secret conundrum. Companies keep adding more security measures to the organisation, but economic espionage and trade secret theft continues to increase unabated. Companies recognise the importance of trade secret assets, but companies do not focus on trade secret identification and classification of trade secrets assets before implementation of security measures not reasonably tailored to protect the specific trade secrets. There is no audit trail, no ownership, and no documentation.

In the EIU study, 13% of the senior corporate executives identified the failure of the organisation to categorise intangible assets is a significant threat to the security of the organisations's trade secrets.

In addition, 22% of the senior executives responded that one of the biggest obstacles to safeguarding trade secrets is "difficulty in defining trade secrets" and 28% that identified a "lack of in-house experience or awareness about trade secrets" as a major impediment to protecting trade secrets.
These are alarming findings especially when one considers the damages caused by trade secret misappropriation. The senior executives identified these consequences of trade secret theft to the organisation: loss of business (52%); loss of competitive advantage (51%); reputational damage (42%); disruption to operations (37%); legal costs (33%); decreased incentives to innovate (22%).

The next step?

Automated Trade Secret Asset Management: Blockchain Metadata

The organisation should focus on the identification and classification of trade secret assets using an automated trade secret asset management system that captures and blockchains the trade secret metadata to establish the existence, ownership, notice and access ("EONA") proofs in a trade secret misappropriation lawsuit.

An alleged trade secret asset is a litigation right. There is no government certification (at this time) for trade secret assets. A trade secret must be proven by documents, contracts or sworn testimony. The same is true for proving the threatened or actual misappropriation of the alleged trade secret asset.

Time is of the essence. A trade secret once lost is lost forever. Delaying the identification of the alleged trade secrets until after the lawsuit is filed results in millions of dollars in wasted discovery and eradicates the obligation of the trade secret owner to develop internal trade secret asset management systems for the identification, classification, protection, and valuation of trade secret assets.

An automated TSAM sotware system captures the *metadata* relating to a trade secret not the actual trade secret. The TSAM system captures metadata about the trade secret like a card catalog in a library the contains the name of the book, the name of the author, the year the book was published, the topic of the book, and the location of the book in the library.

Likewise, the TSAM system captures metadata about the trade secrets including the EONA proofs in a 'blockchain'. A blockchain is a computerised ledger that records and translates trade secret metadata into an encrypted hash code with a digital timestamp called a 'block' that can then be linked to other information in the next 'block' going forward in chronological order. A blockchain provides an efficient, cost-effective, reliable and secure system for managing trade secret metadata with a timestamp function built into the blockchain.

The litigation of trade secret disputes is fact-intensive. The existence of a trade secret is a question of fact; the ownership of a trade secret is a question of fact; evidence of the alleged misappropriator's notice and access to the alleged trade secret is a question of fact and evidence of threatened or actual misappropriation is a question of fact.

Blockchain evidence can drastically reduce or eliminate material issues of fact in a trade secret misappropriation lawsuit saving the parties millions of dollars in discovery. The next revolution in intellectual property law will be the deployment of automated trade secret asset management systems to capture and blockchain trade secret metadata that will unleash and fuel the economic growth of intellectual property assets in the 21st century.

R. Mark Halligan is a highly respected trial lawyer in the intellectual property bar. Mark is a Past-President of the Intellectual Property Law Association of Chicago (IPLAC) and he is the General Editor of the Intellectual Property Handbook published by the Illinois Institute for Continuing Legal Education (IICLE).

Chambers USA ranks Mr Halligan as one of America's Leading Lawyers for Business for his exceptional standing in intellectual property law; Managing Intellectual Property recognises Mr Halligan as an "IP Star." Legal 500 has inducted Mr Halligan in the Legal 500 Hall of Fame for trade secret litigation.

In 2014, Mr Halligan joined FisherBroyles, LLP, as an intellectual property lawyer and litigator. FisherBroyles, LLP is the first and largest distributed, full-service law firm partnership. FisherBroyles, LLP has grown to over 250 partners in 23 offices, all veterans of the largest and most sophisticated law firms, corporate law departments, and government agencies in the United States (and recently a new office in London). This bench strength provides Mr Halligan with stellar resources to litigate or defend trade secret misappropriation cases in the United States with greater efficiencies and lower hourly rates.

Although Mr Halligan is known for his trade secrets expertise, he is also widely recognised by the bar as a preeminent trial lawyer in other intellectual property matters including patents, copyrights, trademarks and related antitrust and licensing issues.

FisherBroyles®
A Limited Liability Partnership

For more information please contact:
rmark.halligan@fisherbroyles.com
+1 312 607-0102