REPRINT

R&C risk & compliance

TRADE SECRET RISK MANAGEMENT IN 2023

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-AUG 2023 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

HOT TOPIC

TRADE SECRET RISK MANAGEMENT IN 2023

PANEL EXPERTS

Mary Guzman
Chief Executive & Founder
Crown Jewel Insurance
T: +1 (404) 290 8155
mguzman@crownjewelinsurance.com

Mary Guzman is an insurance industry veteran and pioneer. She has over 30 years' brokerage experience advising clients on myriad risks to their businesses, most recently with a focus on all things related to technology, cyber, media and intellectual property. She is an industry trailblazer, and one of the first in the industry to develop and sell cyber insurance in 2000. Crown Jewel Insurance is the world's first trade secret insurer.

Bridget O'Connor
Partner
Fortalice Solutions LLC
T: +1 (877) 487 7030
E: bridget@fortalicesolutions.com

Bridget O'Connor is a seasoned operations and management professional responsible for Fortalice's operations and recruiting. For Fortalice, she serves as a stabilising force managing the organisation's growth objectives, including employee hiring and retainment, while representing the firm to clients and business partners with her dynamic, personable and professional 'white glove' style. Fortalice is a global, industry-leading cyber security solutions firm.

Matthew Kohel
Partner
Saul Ewing LLP
T: +1 (410) 332 8710
E: matthew.kohel@saul.com

Matt Kohel is a partner at Saul Ewing LLP and represents clients in commercial litigation, intellectual property (IP) matters and product liability cases. His experience with IP matters includes claims for the misappropriation of trade secrets, trademark infringement, false advertising, the sale of counterfeit goods and cases involving a variety of patent issues, such as inventorship disputes and claim construction.

R&C: How would you characterise the rising importance of trade secrets to company value?

Guzman: In today's digital and artificial intelligence (AI) economy, up to 90 percent of the value of the S&P 500 is in intangible assets. Though not all intangible assets are trade secrets, trillions of dollars of that value may qualify as such. Trade secrets can be the most valuable asset or combinations of assets a company has, as many intangible assets in today's economy are either not patentable from a practical or legal standpoint, or are better left 'secret'. For earlier stage companies that are banking on a critical innovation to get them funding or a buyer, they can be the main driver of that value. Although these assets are, in the US, lumped into 'goodwill', having them valued by an independent third party can increase the value of a company overnight. In an economy run on software code, designs, formulas, business processes, algorithms and AI, it is easy to see that the value of these assets is critical.

O'Connor: Trade secrets and proprietary information are a vital component of an organisation's value in today's business and technology landscape. Trade secrets can provide a significant competitive advantage by offering exclusive knowledge, techniques, processes or formulas that are not readily available to competitors. Organisations can leverage trade secrets to differentiate their products or services, enhance operational efficiency and gain market leadership. Additionally, trade secrets often result from extensive R&D efforts. Organisations invest resources into creating and refining trade secrets and proprietary information that gives an edge in the market. Finally, as organisations operate in global markets, concerns regarding trade secret and proprietary information theft and misappropriation have increased. Protecting trade secrets from foreign governments and industries has become crucial to safeguard.

Kohel: Companies of different sizes, industries and stages in their lifecycle recognise the importance of protecting their trade secrets. One recognised benefit of trade secrets is that this form of intellectual property (IP) can be broad and essentially any type of information that provides a company with an economic advantage. Similarly, the independent economic value of a trade secret can be 'actual or potential' under the Defend Trade Secrets Act (DTSA). Thus, information may qualify as a trade secret even if it may only potentially provide a competitive advantage to a company. In addition, there is no specific way to protect trade secrets that applies to all companies and all situations. Companies may place value in the flexibility afforded

to protecting trade secrets and utilise a variety of reasonable measures to maintain the secrecy of that information.

R&C: What are the potential consequences if a company's proprietary information is lost, stolen or misappropriated?

O'Connor: The loss of proprietary information can give competitors access to valuable trade secrets, IP or sensitive data. This can lead to a significant competitive disadvantage as competitors may use the stolen information to develop similar products or gain insights into the company's strategies and operations. Proprietary information is often a result of substantial investment in research, development and innovation. If it falls into the wrong hands, the company could suffer financial losses due to the devaluation of its IP, loss of market share or decline in sales. In addition, the loss or theft of proprietary information can damage a company's reputation, especially if customers' personal data or confidential business information is compromised. The public perception of a company's ability to protect sensitive information can be significantly impacted, leading to loss of trust and credibility. There are also legal and regulatory consequences. Depending on the nature of the information and applicable laws, the company may face legal repercussions. IP theft can lead to lawsuits, damages and injunctions against the company. Additionally, if the company is subject to industry-specific regulations or data protection laws it may face fines and penalties for failing to adequately protect the information. Finally, if proprietary information is lost or stolen, it can disrupt the company's operations. The company may need to invest time, effort and resources into investigating the incident, mitigating the impact and implementing new security measures, diverting attention from core business activities and resulting in delays or inefficiencies.

Guzman: For corporate trade secrets, the consequences can lead to a devastating loss of customers and market share and overall company value, as well as damage to reputation and stock price, little of which is insured today – although there may perhaps be some narrow coverage under a cyber or directors & officers (D&O) policy. That means that investors and company owners are left holding the bag, with the only possible recourse being very costly and time-consuming litigation – on average $4.2m and 2.7 years if a case goes to trial. If the asset owner does not prevail, then those costs are sunk. Most companies are not adequately prepared to get an emergency injunction or ex parte seizure to try to get their trade secrets back before significant and irreparable harm is done or successfully pursue

damages on the back end. In the worst cases, this could result in bankruptcy.

Kohel: The potential consequences of the loss or misappropriation of trade secrets could be financially devastating to a company. Of course, the best example would be the damage done if the well-protected recipe for Coca-Cola were improperly taken or disclosed. There is an important distinction between the misappropriation of trade secrets and the infringement of other types of IP, specifically, patents, copyrights and trademarks. That is, if a defendant infringes a patent, for example, the patent owner still has rights in the invention for the life of the patent. By contrast, if a bad actor publicly discloses a trade secret, the proprietary nature and economic value provided by that information could be lost forever.

R&C: In your experience, do companies do enough to protect their trade secret assets? To what extent do they fully appreciate what trade secrets are and how they interplay with patents?

Kohel: In my experience, companies employ different measures to protect their trade secrets. Generally, smaller companies and family-owned business may neither be aware that they must take reasonable measures for their confidential information to qualify as a trade secret, nor have a sense of what forms those reasonable measures can and should take. In addition, companies may not appreciate that trade secrets can encompass strategic business information, including beyond customer lists. Conversely, I have found that companies with robust patent portfolios understand the interplay between patents and trade secrets and are likely to have sophisticated IP management strategies that leverage these valuable assets in conjunction with each other.

> **"Not only should a company identify the information it considers a trade secret, it also should understand where that data is kept and how it is maintained."**
>
> *Matthew Kohel, Saul Ewing LLP*

Guzman: The vast majority of companies do not have a formal process to identify, value and mitigate risk around theft of trade secrets. Several factors,

including a culture of an overwhelming focus on obtaining patents, a lack of understanding of what a trade secret is and the legal protections afforded to trade secret owners, as well as a misconception that trade secrets cannot be 'valued', are all contributing factors. Because most companies do not identify their trade secrets, or the assets they want to protect as trade secrets, they cannot apply the appropriate remaining steps of any sound risk management process. These include valuing the risk, implementing proper mitigation strategies against that risk – the higher the value, the more protection necessary – and then transferring the remaining risk, if possible, either contractually or through insurance. Most companies today are simply not doing these things. The final step is to be prepared to mitigate losses when they do occur, which is becoming a bigger challenge every day for companies that have not identified and documented what their trade secrets are.

O'Connor: Organisations and companies should always do the most necessary to protect their trade secrets and proprietary information. Organisations can adopt zero trust principles when it comes to protecting their trade secrets and proprietary information. Zero trust emphasises a 'never trust, always verify' approach and assumes no user or device should be inherently trusted. While zero trust principles have roots within cyber security, this framework can be adopted to protect trade secrets and proprietary information. Some key practices could be utilising multifactor authentication (MFA) and strong authentication to validate the identity of the user, ensuring users and devices with only necessary rights and privileges are provided to do specific tasks, and continuously monitoring user and device behaviour to detect any security threats.

> **"The loss or theft of proprietary information can damage a company's reputation, especially if customers' personal data or confidential business information is compromised."**
>
> *Bridget O'Connor, Fortalice Solutions LLC*

R&C: How much attention are legislators and regulatory agencies paying to trade secrets? Would you highlight any key developments in this area?

Guzman: The Economic Espionage Act (EEA) and the DTSA were passed years ago, and there was a presidential Executive Order in January 2023 demanding sanctions against people and companies outside the US that misappropriate trade secrets, but these tend to focus on the aftermath of trade secret theft – the 'stick'. From an anticompetitive standpoint, there are at least two bills on the floor of Congress right now that would prevent non-competes following the Federal Trade Commission's (FTC's) lead. The perhaps unintended consequence of such a ban would put trade secret misappropriation risk front and centre because employees will feel emboldened to take confidential information with them when they go to a competitor, leaving the former company flatfooted if they were overly reliant on these documents as their key means of protection. Many companies fall into that category. On the other hand, regulatory authorities like the FTC and the Securities and Exchange Commission (SEC) seem to have very little, if any, focus on the value of trade secrets, and their importance to the US economy and to investors overall. I am not sure why, other than that the climate crisis and diversity, equity and inclusion (DE&I) issues seem to have taken the energy at the moment, in addition to privacy, which has been a major issue now for more than a decade. If non-competes are banned, then regulators will have to pay much more attention to the risk to the US economy, and particularly critical infrastructure companies where many of these assets are borne, otherwise companies – including their boards and investors – will not be prepared for what hits them. We need a 'carrot'.

O'Connor: Currently, in the US, the federal government protects trade secrets under the EEA. The EEA makes theft and misappropriation of trade secrets a federal crime. Conviction under the EEA can result in a fine of up to $250,000 for an individual – up to $5m for a corporation – and imprisonment of up to 10 years. If the crime is committed for the benefit of any foreign government, the penalties increase. In 2016, the DTSA was passed, which extended the EEA to include civil trade secret misappropriation claims on the federal level, provides a single uniform cause of action for trade secret misappropriation, and granted legal immunity to whistleblowers. A criticism of the DTSA is that a uniform approach will not meaningfully cover all trade secrets due to rapidly evolving technology. Finally, the European Union (EU) has similar laws to the US through the Trade Secrets Directive. Legislators and regulatory agencies need to stay aware of emerging challenges in trade secret protection due to the increasing rise of cyber security threats and geopolitical challenges across the world. There needs to be a growing focus on addressing these challenges and updating legal

frameworks to address new, evolving risks. It is important to note, the DTSA does not protect the US from foreign governments stealing trade secrets or IP.

Kohel: It is beyond dispute that legislators in the US and the EU understand the value provided by trade secrets. In 2016, Congress passed the DTSA and the EU's Trade Directive went into effect. Earlier this year, the FTC announced proposed rulemaking that would prevent employers from using non-compete agreements. This obviously would have significant implications for trade secret owners, because companies could not stop former employees from working for a competitor. As a result, companies would have to refocus on other means to protect their trade secrets from unauthorised use or disclosure, such as maintaining a robust information security infrastructure, confidentiality agreements and employee training.

R&C: How should companies go about identifying and valuing their trade secrets?

O'Connor: Companies should begin by identifying and classifying the company's IP assets, including potential trade secrets. The classification of IP assets and trade secrets could include customer lists, manufacturing processes, formulas, algorithms,

business strategies or other business strategies, or other confidential information that provides a competitive advantage. After identifying and classifying the proprietary items, evaluate the measures in place to protect trade secrets. Consider factors such as access controls, confidentiality agreements, and restricted physical or digital access. By assessing the security, any gaps or weaknesses in the protection of trade secrets are recognised, allowing the company to take appropriate actions to strengthen security. To determine the value of trade secrets, consider factors such as the cost and effort required to develop or acquire the information. Evaluate the impact of the trade secrets on the company's revenue, market position, customer base and future growth prospects. Finally, conduct periodic reviews of the classification, security and valuation of proprietary information and trade secrets. As the company evolves and new technologies or business practices emerge, the value and relevance of trade secrets may change.

Guzman: First, an internal, cross-functional group including legal, engineering, R&D, HR, risk management and operations, should come together with a list of potential trade secrets, starting with the most obvious and valuable clear drivers of competitive advantage. The group could use an external facilitator experienced in the 'six factor litmus test' and today's definitions – perhaps using

the DTSA definition – of what constitutes a 'trade secret' to guide the discussion on what assets qualify and where to focus the most protection. Perhaps without a workshop but at least as a next step, the company should implement an automated, blockchain software platform which will be critical for future evidence. It will track changes, or 'negative know-how', of the asset as it becomes more valuable, less valuable or obsolete, or is filed for patent protection at which time it becomes public and no longer a trade secret, unless sealed. There are tools available now, and with the inclusion of AI and machine learning language the searches for this data will become easier. As these assets are being tracked, stakeholders can track time and cost associated with each project and trade secret, adding capital expenditures to help ascertain the development cost. They can then use a third party IP valuation expert to assist with the future value of the asset over its expected life. These valuations are typically done on entire portfolios but can be done on individual assets.

Kohel: Because trade secrets may be broad or based on compilations of data pulled from different sources, and are not particularised in a publicly filed application, companies should take a holistic approach to identifying their trade secrets. A company should assess and identify the various categories of information that it believes gives it an advantage over its competitors. That can be both technical information, such as formulas, processes or software code, as well as business information that provides a competitive edge in the marketplace. Not only should a company identify the information it considers a trade secret, it also should understand where that data is kept and how it is maintained. This will enable the trade secret owner to implement the reasonable measures needed to protect its IP.

R&C: Could you outline some of the key steps companies need to take in order to protect their trade secrets? What risk management policies need to be considered?

Guzman: There are several steps in a sound risk management process, the first of which are identification and valuation. Once that is done, the most important thing is to apply countermeasures to the risk based on the likelihood and potential severity of a loss to that asset. Trade secret laws use the term 'reasonable measures' to describe what has to be done to keep an asset secret, which is vague to a fault. While reasonable measures may vary depending on the nature of the trade secret and the size of the company, they should involve best practices, such as the use of non-disclosure agreements (NDAs) and non-competes where permissible by law, new hire guidelines, training and

employee termination practices, exit interviews and related documentation, making those employees and third parties with access aware of the existence of a trade secret. They should also include physical access controls, protection and seclusion, technology access controls, data loss prevention policies, cyber security controls, and documented evidence.

O'Connor: To mitigate the potential consequences of stolen trade secrets and proprietary information, companies should invest in robust security measures, including data encryption, access controls, employee training, monitoring systems and incident response plans. First, adopt a proper vulnerability management programme. Utilising a thorough, risk-based vulnerability management programme should bring awareness to threats and exposures that can negatively impact the organisation. Second, use MFA on email and remote access. MFA is a critical component to reducing risk in an organisation. Third, harness endpoint protection. Utilise an endpoint protection platform to detect and prevent security threats on an endpoint device. Finally, implement security awareness training programmes. Educating all staff within the organisation can help to mitigate risk and highlight the warning signs of a potential cyber threat or attack. It is crucial to prioritise cyber security and create a culture of vigilance and responsibility regarding the protection of trade secrets and proprietary information.

Kohel: A company that values its trade secrets should utilise a comprehensive approach to protecting this information. One such step is to have written standard operating procedures that, for example, emphasise the importance of protecting the company's IP and confidential information, explain when non-disclosure and confidentiality agreements with vendors and other external parties must be put in place, and advise personnel to consult counsel when significant issues arise. Policy implementation should be followed up with regular employee training. In addition, a company should

> **"Without insurance, the assets owner's only recourse is litigation, which can be extremely costly, time consuming and has an uncertain outcome."**
>
> *Mary Guzman, Crown Jewel Insurance*

have the necessary legal, physical and electronic controls in place to protect their trade secrets. Legal measures include contracts with employees and third parties relating to the identification, development, use and disclosure, and ownership of trade secrets, as well as indemnification provisions that protect the trade secret owner's interests. Physical controls can be wide-ranging and include locking offices and desks where trade secrets are kept, security cameras and requiring that visitors be escorted when on site. Also, electronic controls may involve a substantial information security programme that provides employees with access to trade secrets on a 'need to know' basis, such as segregated servers and network drives that are accessible by employees in certain departments.

R&C: To what extent can insurance play a role in protecting valuable intangible assets, including trade secrets? What level of legal and technical coverage does insurance offer?

Guzman: There may be limited coverage available under the company's crime, property or cyber insurance policies for some 'intangible' assets and the cost to replace the data. However, it is not the intent of any of those policies to cover the value of IP assets, as the 'valuation' clause and the exclusions need to be reviewed carefully. There are some new standalone insurance programmes that cover trade secrets on a first-party basis by insuring them at an agreed value. Insurance can fund the costs of investigation and injunctive relief against the misappropriating party, fund the attempted recovery of the asset, indemnify the company for the agreed value of the trade secret if it cannot be recovered, and subrogate on the back end which becomes litigation for damages. Furthermore, as is the case with cyber insurance, simply completing the application process can help a company confirm the value of its trade secrets and gain benefit from a more robust assessment of its potential vulnerabilities. Without insurance, the assets owner's only recourse is litigation, which can be extremely costly, time consuming and has an uncertain outcome.

O'Connor: The level of legal and technical coverage provided by insurance policies can vary. Some policies may offer coverage for legal expenses, including attorney fees, court costs and potential damages awarded in trade secret litigation. Additionally, policies may cover technical assistance, such as forensic investigations to identify the source and extent of a trade secret breach or misappropriation. Cyber insurance could also play a role if trade secrets are misappropriated as a result of a data breach or hacking. Cyber insurance may cover costs such as forensic investigations,

legal fees, notification and services for affected individuals, and potential liabilities arising from the incident.

Kohel: Insurance can help a company deal with the financial consequences of a potential misappropriation of its trade secrets. In particular, an insurance policy could cover the cost of the investigation to determine if there has been an unauthorised access or use of trade secrets and the scope of the issue, as well as pay the legal fees to recover damages and seek other relief in court. In addition to defraying these costs, an insurance policy might pay the trade secret owner the fair market value of the IP lost because of the misappropriation.

R&C: What are your predictions for the trade secrets landscape through 2023 and beyond? As threat vectors change, how important is it for companies to regularly review and update their protection strategies?

Guzman: Trade secrets are the unique know-how that provides a company with its competitive advantage. They are among the intangible assets that collectively make up a significant and growing proportion of the overall value of most modern businesses – rising from 60 percent of total value of the S&P 500 companies 20 years ago to 90 percent today. The velocity of technological change and innovation warp speed contributes greatly to the need for IP strategies that include trade secrets. Trade secrets have many advantages over patents and are becoming a more necessary part of a robust IP strategy of every company. Trade secrets do not have to undergo an 'approval' process, never expire, as long as they are secret, cannot be readily reverse engineered, and the law provides for very robust protection of these assets. Because they are not 'registered' they are never available for public or competitor view, and they cost nothing, other than security measures, to register or maintain in various jurisdictions around the globe. Even if a patent is approved, infringement may occur, leading once again to costly and sometimes fruitless litigation. Couple this with the fact that there is a major push toward banning non-compete agreements, and the environment is bound to be rocky. If companies can no longer use blanket NDAs – as 'de facto' non-competes – they will need to deploy much better tactics to manage their trade secret risks.

O'Connor: As AI evolves, risks regarding trade secrets will increase. With the emergence of 'deepfakes' it may be theoretically possible for a 'person' to be generated by AI, to look and act authentically to steal or manipulate companies into disclosing trade secrets. As social engineering tactics become more sophisticated, organisations

can be exposed to social engineering campaigns that can infiltrate an organisation and steal trade secrets. Those stolen trade secrets could be shared on the dark web or could be used in a ransomware campaign. It is vitally important for organisations to regularly review and update their protection strategies. Creating a culture of vigilance and responsibility regarding the protection of trade secrets will only further protect the organisation as a whole.

Kohel: Trade secret owners will continue to be impacted by the threats of both external and internal bad actors. The seemingly relentless efforts by hackers and the damage that can be done by unauthorised access to a server with sensitive business information demonstrates the importance of maintaining well-developed information security systems and protections. A company's trade secret security procedures should apply to its employees as well. For example, it is good practice to memorialise and implement exit plans for the company to retrieve its electronic devices and proprietary information from departing employees. Separately, the trade secret landscape is going to be significantly impacted by the increasing use of AI to drive innovation. A recent decision by the Federal Circuit affirming the rejection of patent applications that named an AI system as the 'inventor' is going to drive companies to the protections afforded by trade secret law to innovations created by AI.

R&C: In your opinion, what can regulators or legislators do to focus companies on the very real threat of trade secret theft?

Guzman: We need much more focus on prevention and notice to shareholders and investors of what the real risk of trade secret theft is, similar to the pattern we have seen develop in cyber and privacy law. Perhaps even better would be some focus on the 'carrot', such as tax incentives for implementation of formal trade secret asset risk management (TSARM) programmes. Why should we care so much about how a company protects these assets? Because they represent huge value which can evaporate overnight if those assets are no longer secret, and shareholders are none the wiser, and because many of them are in critical infrastructure industries such as green energy, autonomous vehicles, pharmaceutical, defence, healthcare and transportation, which keep us and our planet thriving. R&C