CROSSING THE BORDER: INVESTIGATING TRADE SECRET MISAPPROPRIATION INTERNATIONALLY

Ana San Luis, Davin Teo and Phil Beckett of Alvarez & Marsal create the ultimate guide to protecting company data, detailing what to do when challenges arise

E-commerce and globalisation trends mean that more business owners are likely to move data and conduct business across borders, especially in a post-pandemic world where remote work has become the new norm. When they do so, they should have a firm handle on how to protect their intellectual property, including trade secrets – especially given that the treatment of these can vary widely between countries.

With this in mind, we have set out measures to help companies proactively protect their data, overcome the biggest challenges in conducting cross-border investigations related to trade secret misappropriation and define the best practices from a digital forensics perspective for investigating and remediating breaches in the occurrence of trade secret misappropriation.

How to proactively protect company data

Data surrounding trade secrets is the lifeblood of an organisation and must be treated as critical. Employees at all levels must understand the importance of trade secrets, intellectual property and the dangers of failing to properly secure company data. Assume that all confidential information is at risk. If confidential information is leaked, whether intentionally or not, a company could lose its competitive advantage, as well as millions of dollars – at worst, it could go out of business entirely.

For information to qualify as a trade secret, the information must be known to only a limited group of individuals and reasonable steps must be taken to keep said information secret. Before taking these steps, organisations should consider three perspectives that can greatly enhance the effectiveness of their data governance, security and protection policies:

- The process perspective – classify types of information within concentric rings of importance to the business, balancing security with access to data. For instance, make the most critical data most secure with highly restricted access and make less important information more readily available. Establish the level of control by the roles and responsibilities of staff.
- The human perspective – deploy intensive training to educate employees on how to safely handle company information and reduce the potential for data leaks. Using personal emails to send sensitive company data or transferring data to personal thumb drives are two common examples of poor data control.
- The technology perspective – apply different security levels, access, firewalls and monitoring to track and control how employees can connect with and move the data. Technology can restrict access but can also be used to balance security with usability. Achieving the right balance requires a clear understanding of the value of each type of information.

Armed with these three perspectives, organisations will be better equipped to design and implement the most effective and efficient policies to ensure their data is safe and secure globally.

Maintain well-documented, consistent data governance and security policies

Protecting and securing sensitive company information starts with thoughtful, well-documented and consistent data governance and security policies. Before companies can effectively secure their data, they should understand:

- the different types of data they possess;
- where their data might be located;
- who might have access to their data;
- why one type of data might be more important than another; and
- how data might be accessed and breached.

This will help them understand their various risk levels associated with each type of data.

With the process perspective in mind, an organisation should identify, classify and flag higher risk and sensitive data, such as intellectual property, financial, or mission-critical data but also personal identifiable information and medical information, if applicable. These data type and risk classifications will help inform and drive more effective and robust data governance policies. Such policies should then be implemented to address, manage and secure all types of data based on their risk classifications. These policies should be well documented and applied as consistently as possible across all divisions and entities, while maintaining compliance with local data privacy laws and restrictions, especially for those with a global footprint.

Considering the human perspective, a company should implement NDAs to prevent employees and business partners from passing along a company's confidential information. Similarly, the implementation of NCAs or clauses can prevent staff, contractors or consultants from competing with the organisation upon employment or service termination. Additionally, to help proactively protect company data, a company's policies should be reinforced by regular training and education programmes. These policies should aim to educate both employees within the company and any third parties such as contractors or consultants who may need to access company information.

These policies are critical to demonstrate that an organisation has put initiatives in place to enforce trade secret protection and that those who handle the data are contractually bound not to share the information.

"If confidential information is leaked, whether intentionally or not, a company could lose its competitive advantage, as well as millions of dollars – at worst, it could go out of business entirely"

Create and sustain robust IT security infrastructure

With the technology perspective in mind, technology can greatly enhance a company's ability to safeguard sensitive information while allowing employees the access they need to fulfil their responsibilities. The goal is to prevent data loss. Security tactics are required to address both external threats and internal security gaps. Some companies are more prone to external threats and others to internal issues because of lax policies, but both are related. An external hacker may use phishing techniques to coax employees to unwittingly give out sensitive information that the hacker can use to skirt firewalls and access company data.

Some of the primary initiatives that companies can take to improve their IT security infrastructure include the following:

- Data loss prevention – use technology to safeguard data in three areas. Data used by employees, information transmitted or transferred (eg, to another internal entity) and data at rest, such as databases, file-sharing sites, data in the cloud and any storage devices allowed by local data privacy regulations.
- Encryption – establish encryption technologies and protocols to protect passwords, data and storage devices. Implement measures to ensure a minimum threshold of strong password security where individuals are asked to provide them.
- Two-factor authentication – enable two-factor authentication across core business systems to ensure that they are protected by an enhanced level of protection.
- Permission checks – deny permission to any users violating company policies, such as sending sensitive information outside the organisation to a personal account.
- Unauthorised transfers – prevent data transfers to and from external devices (eg, USB thumb drives) by disabling the ability for company-owned devices to read from or write to external ones. Disable employee access to non-company, cloud-based websites and mobile apps to prevent unsanctioned data transfers via the cloud.
- Email monitoring – use technology to scan incoming emails for potentially malicious attachments or suspicious links.
- Disabling devices at termination – immediately disable terminated employees' access to all company systems, initiating a remote wipe of company data when company-owned devices are not returned.
- Mobile device management – secure, control and enforce policies on smartphones, tablets, security tokens and other devices, as allowed by law. Strictly manage any accessible or stored company data and prevent mobile data back-ups to non-company cloud accounts or devices.

Enhancing data and cybersecurity should be a company-wide concern. Organisations must be proactive in improving data protection continuously through regular assessments and consistent monitoring. In reactive circumstances, immediate identification of leaks and quick remediation of data breaches are essential to protecting trade secrets and IP assets.

Managing challenges in cross-border trade secret misappropriation

Despite a company's best efforts to protect and secure their data, mistakes and data leaks may still occur, which becomes increasingly challenging when this happens across borders.

One of the biggest hurdles to overcome when investigating such misappropriation is understanding and working around a company's infrastructure for data storage — where data is stored, how it is used, who uses it, what data can be reviewed and how much needs to be collected and reviewed. Large volumes of data stored in tightly controlled environments, or large quantities of data sources and devices scattered across various countries, may complicate the collection and review for a cross-border investigation. In an ideal situation, investigators would be able to gather and review all relevant data in one centralised location. However, because of varying data privacy laws around the world, that has become increasingly difficult, where it is even possible at all. Legislation mandating data protection levels may vary between jurisdictions and countries, leading to access barriers for investigators. In many cases, investigators may be restricted from moving data out of the country and may only be allowed to access data for review on premises.

In addition to understanding potential data storage and access limitations, investigators must also consider the differing perspectives between IT and employees on the handling, usage and protection of intellectual property and company data. Individual employees may have specific requirements to adhere to when using the data to conduct day-to-day business. Understanding both (sometimes vastly contrasting) perspectives can aid investigators in more efficiently reviewing data in cross-border investigations.

Such challenges in cross-border investigations can be overcome by obtaining a clear understanding early in the investigation of the scope of the breach and designing a clearly defined plan of action; one that mobilises, organises and aligns investigative teams in different jurisdictions with appropriate IT resources and stakeholders. On-site investigators may need to prioritise jurisdictions with stricter data privacy and protection regulations to account for longer review timelines. Alternatively, investigative teams may split up to handle different jurisdictions in parallel. Data from less restrictive jurisdictions may be transferred for review to the least restrictive jurisdiction, if allowed, while data from more restrictive jurisdictions may be reviewed on-site.

Below are several other challenges investigators may face in cross-border investigations and how to overcome them.

Lack of resources and protocols to conduct investigations

While companies may have policies in place to proactively protect their data, sometimes they may not have the resources or the protocols in place to reactively handle and investigate data breaches. Companies should clearly define both protocols and those internally and externally who will conduct investigations. Are there enough resources to do the job? Are the right protocols in place to move forward? Companies can improve protocols by regularly performing simulations and exercises to test the robustness and effectiveness of their investigative processes and procedures.

Insufficient compliance with foreign privacy laws and knowledge of local customs

Legal requirements, cultural environments and languages may vary across different countries. Companies should ensure investigative resources have a clear understanding of local cultures and data privacy laws, and how these may differ between countries. Investigators should adjust investigative practices and language used during interviews as needed to account for cultural differences and to ensure questions are being communicated clearly and respectfully. Investigators should also confirm that the collection, handling, storage and transfer of protected information adheres to local regulations.

Poor date and time stamp maintenance

When dealing with data from different geographies, investigators will likely handle data with dates and time stamps originating from multiple time zones. Proper preservation, review and analysis of dates and time stamps can be particularly crucial in trade secret misappropriation matters in proving, for example, that certain files containing trade secrets existed on company A's machines before company B's. Investigators should ensure the proper preservation of document metadata with digital forensic equipment and software to allow for accurate review and analysis. Meticulous documentation, such as chain of custody, evidence notes and acquisition information is crucial. For analysis purposes, investigators should agree to utilise one standardised time zone to minimise manual time zone comparison and conversion errors.

Ineffective remediation across borders

Once trade secret misappropriation has been confirmed, a defensible deletion of misappropriated data from competitors' devices and systems may be ordered. This process must be methodical and repeatable, and demonstrate that the data cannot be recovered later, otherwise the remediation may be considered ineffective. The disputing parties must agree on a defensible deletion process, including specific items confirmed for remediation and the data sources and devices from which to remediate.

Investigation teams should aim to have a diverse range of viewpoints when solving trade secret misappropriation or IP infringement matters. The investigation should not be left solely to the technology resources involved. Perspectives from team members who have broader investigation experience are crucial in guiding, navigating and managing challenges faced in the investigation. These perspectives can include attorneys, fraud experts and employees who consistently use and know the data.

Best practices in digital forensics for trade secret misappropriation

Unless a company has a functional forensic investigation team in place, a misappropriation investigation should not be attempted alone. Too often, inexperienced teams wind up contaminating the evidence and therefore introducing doubt. When data breaches occur, speed is of the essence but not at the expense of an appropriate, disciplined approach.

Evidence gathering and investigation

Whichever team is on the case, ensure that local resources who are familiar with the language, culture, customs and regulations handle or

co-handle and translate for custodian interviews. Custodians are the owners of the data and outside the United States they often have more protection under personal data privacy laws. Interviewers should take care not to cross cultural or regulatory boundaries.

Obtain appropriate permissions and consent from company entities and custodians ahead of time, especially in those countries with strict data privacy laws.

Identify, map and understand all data sources that may have been subject to a breach and establish them as in scope of the investigation. Such data sources may include laptops, desktops, mobile devices, external storage devices, network shares, media, cloud-based applications, chat applications and databases.

Ensure that up-to-date digital forensic equipment and software is used to collect and image all electronically stored information (ESI) in a forensically sound manner, allowing for the accurate preservation of ESI metadata such as dates and time stamps.

Properly handle and securely transfer original evidence, collected data and forensic images according to local data privacy laws. Encrypt data prior to transferring but be aware that some countries may restrict the types of information that are allowed to be encrypted.

When it comes time for analysis, agree on one standardised time zone and continue to apply meticulous documentation throughout the course of review. Take special note of any differences between actual and represented dates and times in the basic input and output system information of electronic devices, where applicable. Properly account for discrepancies in dates and times to ensure that accurate analysis is being performed. Tightly control access to any review databases, maintaining audit logs of who accessed what.

When reporting on the results of a cross-border investigation, understand and comply with any reporting restrictions that may be imposed by specific jurisdictions involved in the investigation.

Remediation

When remediating trade secret misappropriation or IP infringement, establish a confirmed use of unique hashes — the fingerprints for files — to identify agreed-upon items from in-scope data sources and devices. Prepare and run deletion scripts on the devices for only the agreed-upon items.

Document remediated items by using a combination of logs, notes and screenshots where applicable. Avoid impromptu, undocumented deletion of files from target systems.

Finally, re-image and reanalyse all in-scope data sources and devices post-remediation to confirm that the unique hashes for agreed-upon items can no longer be found on the target systems. No remediated or deleted items should be recoverable by data recovery tools or other digital forensic means.

Applying a methodical, well-documented, repeatable and thorough approach to data remediation allows for a successful and defensible deletion of misappropriated data.

Establishing the right team and method up front is paramount

In the end, the amount of effort a company applies up front to prepare for cross-border trade secret investigations will be well worth the time. Companies must handle all information in a forensically sound manner, while respecting and abiding by local customs and data privacy laws. Data breaches and trade secret misappropriations must be addressed in a timely manner and in accordance with the regulations of involved countries.

Equally important is the makeup of the team conducting the investigation. Companies should ensure that they have the depth of resources needed to conduct the investigation and that the team functions collaboratively, so active communication and learning exists across the various areas of the investigation: legal, forensics, finance and engineering, among others.

Establishing well-defined methods of evidence gathering, building a diverse team of investigators and overcoming international challenges will help lead to the most successful and efficient resolution possible for a cross-border investigation. IAM

Phil Beckett and Davin Teo are managing directors and Ana San Luis is a senior director at Alvarez & Marsal (pbeckett@alvarezandmarsal.com)