Cybersecurity and Trade Secret Protection

By Peter Lando and Dmitry Milikovsky

Trade secrets and proprietary information can drive key differentiation and time-to-market in competitive markets. However, the problem in our hyper-connected world is that information, no matter how confidential, is easy to copy and transmit at essentially zero cost. This leads to heightened risk for misappropriation and theft of proprietary information and trade secrets.

Trade secret theft and misappropriation risk is predominantly from people who are either inside or doing business with your company. Statistics show that the more than 90 percent of defendants in trade secret litigation are employees or business partners of the trade secret holders. Technology and an understanding of security standards become very important in trade secret protection due to the continual evolution of the legal definitions of "reasonable steps" or "reasonable efforts," which are required to be undertaken by a trade secret owner to protect and enforce these rights against misappropriation.

Cybersecurity is a major concern for multiple functions of a company as well as for compliance with regulatory requirements in many areas. Generally, IT groups take the lead in crafting and detailing the security policies that protect the critical infrastructure and information of companies. Issues that are often addressed in creating cybersecurity systems include key risk identification, access controls, data handling policies and security tool selection.

Early and continuous involvement by the legal team is helpful for a common understanding of legal requirements for maintaining proprietary information and trade secret protection, and for the legal team to understand the strengths and limitations of the tools available in the market. It also allows the groups to be able to communicate in a shared language and establish cybersecurity procedures that help to effectively protect commercial advantages.

Currently, there are several cybersecurity frameworks and standards that facilitate the creation of information and cybersecurity processes that are used by industry.

> Involvement by the legal team is helpful for a common understanding of legal requirements for maintaining proprietary information and trade secret protection.

CYBERSECURITY FRAMEWORKS AND STANDARDS

Key frameworks for building and maintaining cybersecurity include the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization Standardization (ISO) 27000 series standards.

The NIST Cybersecurity Framework is a suggested approach to create a cybersecurity process, while ISO 27001 — of the ISO 27000 series — is used by independent auditors to certify that an entity has met a requisite level of protecting sensitive company information through physical, environmental, and human resource security and access control. These are both commonly used approaches for creating and implementing best practices for cybersecurity risk management processes. For example, some surveys have found that 84 percent of organizations across a wide range of sizes and industries already leverage some type of security framework. A recent survey by ISO reported that over 31,000 entities had obtained ISO 27001 certification for their information security management system and control processes.

An understanding of the cybersecurity framework and information security guidelines allows legal practitioners to communicate with cybersecurity teams and influence the processes to protect trade secrets and confidential information according to the appropriate legal and regulatory standards. Further, it helps legal practitioners understand the issues and trade-offs in creating viable cybersecurity processes.

The NIST Cybersecurity Framework has five functions, each with several categories and subcategories, which may be used to create and manage cybersecurity processes. The Framework includes activities that may be used to address protection of confidential and proprietary information. It also refers to other standards, including ISO 27001, on how to address those activities that should be part of a given category.

A high-level definition of each of the five functions is as follows:

- **Identify:** Develop an understanding of the cybersecurity risks to be able to manage the systems, people, assets, data and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services and protection of key information to address identified risks.
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event, using the tools, processes and systems that have been implemented to address the identified risks.
- **Respond:** Develop and implement appropriate actions, including involving all the appropriate internal and external stakeholders, regarding a detected cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to restore any capabilities or services that were impaired due to a cybersecurity incident, and that improve existing safeguard processes and tools.

Part of risk identification includes creating cybersecurity governance, which addresses support for compliance with legal and regulatory requirements. This references sections of ISO 27001 that support addressing intellectual property rights protection of both internal and third-party information, and the use of non-disclosure and confidentiality agreements as examples of items that are reviewed to obtain certification under the standard.

In addition, the ISO 27001 standard requires review as to how information is protected from unauthorized access and release. For counsel working with management, a useful initial step would be to work with the IT, business and technical teams to create a process to identify proprietary information and potential trade secrets.

There are tools, such as data security platforms, that search files for specific information used for data classification. They are available as part of cloud provider offerings, and can be used to identify proprietary and trade secret information, especially if application for privacy compliance has already been made. These tools classify documents by searching for key words and using machine learning approaches to improve over time. They can be used to identify items, for example, documents and files — such as those with customer information, technical terminology and confidentiality labels — as confidential, proprietary and potentially trade secret.

THIRD-PARTY RISK

Another important part of the risk identification is to understand and categorize suppliers and third-party partner information systems. The objective is to ensure protection of assets that are accessible by suppliers and partners. As is common practice, confidentiality provisions should be included in supply, evaluation, development and similar agreements. However, access to proprietary electronic information should be addressed both from a contractual and an electronic security standpoint.

There are number of technologies that can provide this functionality. Pro-

continued on page 35

Trade Secret Protection

continued from page 31

viding these requirements to the cybersecurity personnel can lead to the best tools and process for the organization. These solutions, which are also part of data protection platforms, provide partner access and employee access controls, and track access to applications, documents, files and directories by employees and contractors.

The protect function includes activities to develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. One of the requirements of this function is having and maintaining access control systems. It provides references to portions of the ISO 27001 standard that require creating a detailed and documented access control policy, which is to be periodically reviewed. The access control policy addresses assigning or revoking access rights for all users to all systems and services available based on business requirements.

In creating an access control policy, it is useful to review both the information identified as being proprietary during risk identification and additional information that is later identified by a data security platform or otherwise. Specifically, thought should be put into: (1) which users have access to proprietary information; (2) whether users that have access to proprietary information should be able to access it remotely or via personal devices; (3) how to grant access to proprietary information on an ongoing basis; and (4) how to grant access to proprietary information in third-party discussions, for example, triggering legal or NDA approval for sharing information that is identified as proprietary.

User access control frameworks can take many forms. These include employee role-based access control; creating categorical levels of access to certain information, which requires different approvers at each level; having separate read, write, copy and execute permissions; and wholesale limitation to the ability to copy and transmit certain files or documents. The culture and business processes of an organization are important factors in how user access is granted and changed.

The culture and business processes of an organization are important factors in how user access is granted and changed.

In addition, both the NIST Framework and ISO 27001 require that all employees and contractors receive appropriate awareness training, which should include regular updates of the relevant policies and procedures. This training is a great tool for informing employees of their obligations for proprietary information and obtaining feedback to improve the process and find information that may have been missed or that may be problematic in being maintained as confidential. Further, it can be used as evidence that notice of protection of trade secrets and confidential information was communicated and shared with company personnel.

Both the NIST Framework and ISO 27001 require that log records are determined, documented, implemented and reviewed periodically according to a detailed process. These logs can be used to determine when proprietary information may have been transmitted inappropriately and allow expeditious action to be taken. Further, the documented processes and log records can be used to bolster a showing that reasonable measures have been taken to protect proprietary information.

Additionally, ISO 27001 requires that managers regularly review the compliance of information processing and procedures within their area of responsibility with appropriate security policy standards. It would be useful for legal counsel to evaluate access logs to proprietary and potentially trade secret information as part of the periodic review. This allows for understanding frequency of use and determining whether there are issues that need to be identified. Further, if machine learning is used for anomaly detection, labeling any events as problematic, non-problematic or with additional categories can speed up improvement of these machine learning algorithms.

The information security management processes of the NIST Framework and the ISO 27000 series standards are widespread and leading best practices for cybersecurity, and can be used to create and document measures taken to protect trade secrets and proprietary information. Understanding that the NIST Framework and information security guidelines are useful tools that can help counsel to participate in and influence activities and discussions with the teams that develop, manage and implement cybersecurity processes. ■

Peter Lando is a founding partner of Lando & Anastasi, LLP, an intellectual property boutique law firm. His practice involves all areas of intellectual property and related transactions.
Plando@LaLaw.com

Dmitry Milikovsky has over 20 years of legal and business development experience in the consumer electronics, telecommunications and software industries, including as Vice President, Business Development and Licensing at Qualcomm.
dmitry@milikovsky.com