THE IMPORTANCE OF CYBERSECURITY FOR TRADE SECRET PROTECTION

Developments in trade secrets cases and the growing role of the NIST Framework
AN INTRODUCTION

The rising threat of cybersecurity breaches for companies and other organizations puts the confidential technical and business information that gives companies their competitive edge—commonly known as trade secrets—at greater risk from theft and loss. Implementing effective cybersecurity protection is therefore becoming one of the key priorities of companies whose business depends on trade secrets, not just as a practical security matter but also because under U.S. and international law the legal protections that courts will give to a company's trade secrets directly depend on whether the company itself has taken “reasonable steps” to protect that information.

Courts in the U.S. and elsewhere have begun to look at the cybersecurity measures that firms have taken, in addition to other more traditional security and risk management measures, in determining whether confidential information has been protected adequately enough to be considered a trade secret. Recent developments in cybersecurity protection among industry and governments, particularly the NIST Cybersecurity Framework in the U.S., are also helping to define voluntary cybersecurity measures that undoubtedly will be looked to in future trade secrets cases as relevant “reasonable steps” for securing trade secret protection. This whitepaper will survey these cybersecurity trends in trade secrets cases and NIST Framework developments.

Protecting trade secrets is not just an information-technology security issue—the other people and process risks to trade secrets at a company are also of critical importance and need effective assessment and management. Cybersecurity itself is evolving to be more firmly grounded in enterprise-wide risk management and to include many of these types of people and process issues as well. Effective design and implementation of cybersecurity, and the protection of trade secrets more broadly, do have the interrelated and compatible goals of protecting organizations’ value and reducing monetary and reputation risks—and thus need to be managed consistently and effectively across all relevant areas of a company.

FOR MORE INFORMATION
Please visit www.CREATe.org, contact us via email at info@create.org or follow us on Twitter @CREATe_org.
TABLE OF CONTENTS

Overview

I. Cyber Threats to Trade Secrets

II. The Legal Relevance of Cybersecurity for Trade Secret Protection

III. “Reasonable Steps” of Cybersecurity
    1. Identity and Access Management
    2. Data Security Measures
    3. Perimeter and Network Defenses
    4. Communication
    5. Monitoring

IV. Trends in Cybersecurity and Trade Secret Protection: Enterprise Risk Management

References

The content of this whitepaper is for informational purposes only and is not intended to provide and should not and cannot be considered as legal advice or legal opinion.
Increase in cyber incidents year on year: 64%
Companies detecting a breach or hack: 65%
Increase in trade secrets and other IP theft: 56%
Breaches involving insiders: 60%

IBM 2016 Survey of Cybersecurity Landscape¹ Klahr et al., Cyber Security Breaches Survey 2016²
I. CYBER THREATS TO TRADE SECRETS

By any measure, cybersecurity threats and breaches are on the increase. IBM’s 2016 Cyber Security Index report found that the average company surveyed experienced 64% more cybersecurity ‘incidents’ in 2015 than it had the year before. In the U.K., a government sponsored survey in April 2016 found that 65% of large firms had detected a cybersecurity attack or breach in the past year. Cybersecurity is thus becoming a high priority for companies small and large. Morgan Stanley reports that the market for cybersecurity products and services will reach $60 billion in 2016, a figure that could double by 2020.

Trade secret theft is a common objective of cybersecurity attacks, and IBM estimates that there has been a 56% rise in these and other intellectual property (IP) related attacks year on year. In addition to external attacks, electronic misappropriation or transmission of data by internal staff, contractors or other known third parties is a common problem. Indeed, employees and other malicious or careless insiders account for about 60% of all cyber-attacks, which arise from unauthorized access, viruses or other malicious code, ‘phishing’ attempts, and other means.

A number of prosecutions and civil and administrative cases that have arisen this year illustrate the types of cybersecurity risks to trade secrets that companies are experiencing:

- **GSK.** Two research scientists working at GSK were indicted in January 2016 for allegedly downloading and emailing confidential and proprietary data about GSK’s biopharmaceutical products, research data, procedures, and manufacturing processes and sending it to a Chinese research startup company.

- **U.S. Steel.** The company filed a complaint with the U.S. International Trade Commission in April 2016 alleging that a 2011 cyberattack on the computer of a senior U.S. Steel researcher took three gigabytes of confidential information on three U.S. Steel products. The company’s complaint links this cyber breach to the Chinese government.

- **Epic Systems.** Medical software company Epic secured a $940 million jury verdict and permanent injunction against Tata Consulting Services in April 2016 in its case alleging trade secrets and other violations. Epic claimed that Tata unlawfully downloaded more than 1,000 files of confidential information from Epic’s restricted-access web portal, using a third-party licensee’s access, and used this information to develop a competing product.

- **Harry Schein, Inc. (HSI).** Medical supply company HSI secured a preliminary injunction against former sales consultant Jennifer Cook in June 2016 prohibiting her from accessing or disclosing HSI’s trade secrets. Schein alleged that Cook forwarded company customer, inventory, price, and equipment proposal information to her personal email account, kept a company laptop for two weeks after she left the company, and accessed the HSI computer system without authorization after her employment ended.

- **Panera.** Bakery-café chain Panera LLC secured a temporary restraining order in August 2016 prohibiting its former information technology (IT) architect Michael Nettles from working for competitor Papa John’s or using or disclosing Panera’s trade secrets, claimed to include business strategies and confidential innovations. The court ordered Nettles to turn over for inspection his personal laptop and other devices used at any time to store confidential Panera information.
II. THE LEGAL RELEVANCE OF CYBERSECURITY FOR TRADE SECRET PROTECTION

The steps that companies have taken to protect their trade secrets are a vital factor in legal cases brought to address trade-secret misappropriation, given that the legal definition of a protectable trade secret includes the specific requirement that the owner or other holder of the information take “reasonable steps” or “reasonable efforts” to keep that information confidential.

The new U.S. Defend Trade Secrets Act, adopted in May 2016,11 incorporates the definition of trade secrets from existing federal criminal law and protects “all forms and types of financial, business, scientific, technical, economic, or engineering information” where “the information derives independent economic value, actual or potential, from not being generally known [or] readily ascertainable” and where “the owner thereof has taken reasonable measures to keep such information secret.”12

This requirement to take “reasonable measures” to keep a trade secret confidential has long been an element of U.S. state trade secrets laws,13 as well as the federal Economic Espionage Act14 and International Trade Commission unfair competition rules.15 Internationally, a “reasonable steps” requirement is part of the 1996 World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)16 and explicitly or implicitly part of many countries’ national trade-secrets legislation.17

The new European Union Trade Secrets Directive18 likewise protects information that is confidential (i.e. not generally known or readily accessible), that has commercial value because it is secret, and that “has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to secret.”19 This Directive entered into force in June 2016, and requires all EU member countries to harmonize their trade-secrets protection along these lines by June 2018. Several European national laws already contain a “reasonable steps” requirement in their definition of trade secrets.20

How a company or other trade-secret owner protects its trade secrets is thus important not just as a practical way of reducing or preventing theft. If those trade secrets do get stolen, the company will not be able to get legal redress under trade secrets laws if it cannot demonstrate that the steps it took to protect those trade secrets were “reasonable.” Without such “reasonable steps” or “reasonable efforts,” courts can simply find that the information does not meet the definition of a trade secret and thus gets no legal protection at all. For example, a U.S. court recently refused to grant a temporary restraining order against alleged trade-secret defendants in part because the court found that there were “serious questions as to whether [the plaintiff] took reasonable efforts to maintain the secrecy of the information at issue.”21
As “digital misappropriation” of trade secrets increases, cybersecurity measures will take on an added significance in reinforcing the legal protection of companies’ confidential information in many cases. Courts in trade secrets cases have already begun assessing whether various elements of companies’ cybersecurity have been carried out sufficiently well to be deemed “reasonable steps” or “reasonable efforts,” for purposes of deciding whether to give legal protection confidential information that may have been misappropriated by cyber or other means.

This trend is likely to continue as businesses’ internet usage and Cloud storage expand further, and as trade secrets cases focus more frequently on whether companies are taking reasonable efforts to meaningfully achieve the sort of protections online that they have long needed to maintain through physical security on their premises.

Published opinions in trade secrets cases to date have not examined a large number of cybersecurity issues in detail, but the types of cybersecurity that courts have considered mainly involved measures that cybersecurity experts would classify as (1) identity and access management, (2) data security measures, (3) perimeter and network defenses, (4) communication and (5) monitoring.

1. IDENTITY AND ACCESS MANAGEMENT

There are many ways in which companies and other organizations can manage who should have access to their trade secrets in electronic form, and how they should get such access. Courts so far have looked at some very basic forms of identity and access protection in trade secrets cases:

Password protection. Although courts have recognized that password protection is not necessarily sufficient in and of itself to meet the test of “reasonable efforts,” using password protection to control access to confidential information has been mentioned in about 5% of trade secret cases as one of several activities that together warranted giving legal protection to a company’s confidential information.

‘Need to know’ access. Limiting electronic access of particular confidential information to only those employees and others who require such access in order to perform their job duties also can be evidence of “reasonable steps.” In a classic case from 1991, electronics firm Texas Instruments (TI) won a trade-secrets misappropriation case against two former researchers who had copied all of the computer directories to which they had access at TI, which included the speech-recognition programs that TI claimed as trade secrets, and went to join a competing firm. The court mentioned with approval a fairly long list of TI’s “reasonable measures,” which included password-limited access to those directories that was restricted to employees having a “need to know.”

Secure server storage. Courts in trade-secrets cases have also noted some companies’ efforts to secure and sometimes to segregate the storage of certain sensitive trade-secret information on their computer networks, as one element in determining whether that data should be given trade secrets protection.

2. DATA SECURITY MEASURES

Particular cybersecurity protections that deal with how confidential data may or may not be stored and transferred have been cited in a few cases as important “reasonable efforts” in protecting trade secrets, for example:

USB use restrictions. Confidential data often can disappear from a company, and computer viruses and other security-breaching “malware” can be introduced, through the use of portable and personal devices. At least one court case has recognized that policies such as those prohibiting or limiting the use of USB sticks on company equipment can be an important part of “reasonable efforts” to protect trade secrets.
Distribution controls. Not all cybersecurity problems are entirely electronic, of course. The use of company information systems and equipment to print confidential documents for physical removal from the company is a common means of misappropriating trade secrets. A Japanese company’s failure to prohibit the printing of sensitive documents has been mentioned in a court’s list of reasons why that company’s information should not be protected as a trade secret. There are obviously cybersecurity counterparts to physical printing restrictions, such as restricted permissions for electronic distribution, that are also likely to be relevant in future cases.29

3. PERIMETER AND NETWORK DEFENSES

Attempts to access a company’s trade secrets by competitors, “hacktivists,” malicious ex-employees, and even nation states, can take the form of hacking of the company’s external networks or internal equipment. Courts and litigants thus have started to highlight the perimeter and network defenses that companies have put in place as evidence of the “reasonable steps” they have taken to prevent this kind of trade-secret theft:

Firewalls. Companies’ use of network firewalls has been mentioned in trade-secret litigation as a helpful “reasonable step.”30 For example, in a 2016 case involving an alleged improper access and attempted misappropriation of the plaintiff company’s proprietary merchant-management system, the court issued a preliminary injunction against the defendant, noting the plaintiff’s numerous “reasonable efforts” in implementing security measures “including the use of network infrastructure that is protected from outside interference or access by sophisticated firewalls.”31

Data encryption. Maintaining the company’s most sensitive information in encrypted form has been commended by courts as helpful in confirming that the information is in fact a trade secret.32 One U.S. court has found, for example, that a developer’s encryption of its automobile-system performance enhancement software prior to its distribution to the public, and limiting of the encryption keys to authorized distributors and dealers, was a sufficient “reasonable effort” for protecting the developer’s trade secrets.33

Online use restrictions. Malware of various types that pose risks to a company’s confidential information can enter a company’s computer equipment and networks when employees and other IT users access certain untrustworthy internet sites. Some cases to date have noted that blocking user access to certain websites to protect their computer systems from intrusion can also be a “reasonable step” in protecting trade secrets.34

4. COMMUNICATION

Companies’ communications with and training of their employees in cybersecurity and other aspects of trade-secret protection are vital best practices. A few courts have recognized certain types of electronic communications to employees as helpful “reasonable efforts,” for example:

Pop-up warnings. Real-time messages to users when they engage in computer or network behavior that raises risks to cybersecurity or trade secrets, has been mentioned by at least one court as a helpful “reasonable effort” in keeping confidential information secret.35

5. MONITORING

Cybersecurity is obviously not just a one-time exercise in putting particular protections in place for all time, but rather an effort that needs to be monitored, measured and improved over time as incidents arise, technology advances, staffing changes and business models evolve. Courts have started to recognize some elements of ongoing cybersecurity monitoring as relevant for protecting trade secrets:

Email monitoring. Many companies’ personnel and IT policies include a provision that permits the company to monitor and flag-up various types of internet communications done on the company’s equipment and networks, for example, the sending of company material to personal email addresses or cloud services. Such monitoring has been mentioned as a “reasonable step” by courts in some trade secrets cases. In a recent state case in North Carolina, for example, the court found that the plaintiff had stated a valid claim for trade secrets misappropriation, in part due to “reasonable efforts” which included “an electronic communications policy permitting the company to monitor employee communications, in part, to protect against unauthorized disclosure of company trade secrets.”36
Although cybersecurity and trade secret protection are not one and the same thing by any means, they have many similar goals and functions for companies—securing valuable information, encouraging and protecting innovation, protecting value, discouraging theft and disruption, and avoiding unnecessary expense, loss and damage to reputation. It is therefore not surprising that cybersecurity, and trade secrets protection more broadly, are evolving and converging in many ways, in particular to involve more holistic risk assessment and risk management practices throughout companies and other organizations. This trend will not only help to protect trade secrets more effectively from loss or theft in the first instance, but will also help companies demonstrate that they took the sort of “reasonable efforts” or “reasonable steps”—both cybersecurity and other trade-secrets specific protections—needed to ensure legal protection for their confidential and proprietary information.

Cybersecurity standards and best practices are becoming more widely used in the U.S. and internationally. There are numerous cybersecurity standards and practices among different industry sectors, but the International Organization for Standardization (“ISO”) ISO 27001 formal standard is among the most widely used by companies...
82% of U.S. government IT and security professionals are using the NIST Framework to improve security.

70% of private-sector professionals regard the NIST Framework as a leading practice.

*Dell, Dimensional Research & Tenable Network Security*
internationally to assess their cyber objectives and risks, and to implement technical and management-systems protections throughout their organization.\textsuperscript{38} The European Union recently adopted a Directive on the security of network and information systems (NIS) that will require more comprehensive cybersecurity among its national governments and “critical infrastructure” industries.\textsuperscript{39}

In the U.S., the voluntary Framework for Improving Critical Infrastructure Cybersecurity (the “NIST Framework”),\textsuperscript{40} developed by the National Institute of Standards and Technology (“NIST”) unit of the U.S. Department of Commerce, seems to be getting the most widespread support among government and industry sectors as a cybersecurity best practice in the U.S.—and is also getting favorable attention in some other countries internationally. Recent surveys have found that 82\% of U.S. government IT and security professionals are using the NIST Framework to improve their security, and 70\% of private-sector professionals regard the NIST Framework as an industry leading practice.\textsuperscript{41}

The types of identity and access management, data security measures, perimeter and network defenses, communication, and monitoring activities that have appeared piecemeal in the relatively few trade secrets cases that have mentioned particular cybersecurity practices so far, are dealt with in a detailed and structured way among the 5 functions, 22 categories, and 98 subcategories of the NIST Framework.

Some other types of cybersecurity protections dealt with in the NIST Framework that are relevant to trade-secret protection (and indeed to protection of any kind of company data) but that have not featured in trade-secrets cases in any significant degree to date include such activities as vulnerability assessment and management (understanding and managing against potential risks and breaches), configuration management (standard and permitted customizations of company and users’ IT systems), and incident management (response to and mitigation of breaches that do occur). These and other specific approaches and actions recommended in the NIST Framework can not only help a company’s overall cybersecurity efforts, but can also serve as evidence of “reasonable steps” to bolster the case that the company’s confidential information should be treated as trade secrets as a legal matter.

One of the most compelling features of the NIST Framework is that it can help companies think about protecting their trade secrets and other company data in an organized way, based on broader enterprise risk management techniques that focus on analyzing risks, prioritizing risk management steps, and implementing those steps in a consistent way wherever risks to that information might arise throughout the company or other organization.

Many of these types of enterprise risk management steps that the NIST Framework deals with specifically for cybersecurity—for example, having relevant employee and third-party policies in place, training staff and third parties on what is required, managing third parties well, monitoring the company’s cybersecurity implementation, and taking corrective action when an incident takes place—are the types of questions that courts already consider when considering “reasonable steps” in protecting trade secrets more generally: Do employees know what they are meant to do? Have precautions been taken when giving access to third parties? Has the company dealt promptly and consistently with breaches?\textsuperscript{42}

We expect that courts in trade secrets litigation will increasingly consider implementation of various elements of such standards and such industry guidance as the NIST Framework in deciding whether sufficient “reasonable steps” have been taken to protect a trade secret. Although courts have not yet specifically called out the NIST Framework in trade secrets cases, one court has already referred to another cybersecurity standard in the financial services sector—the PCI-DSS standard—as one of a number of protections that together were deemed “reasonable efforts” to protect a trade secret.\textsuperscript{43}

The well-regarded NIST Framework certainly bears consideration as a template not only by which a company manages cybersecurity generally throughout its organization, but also by which it implements its “reasonable steps” for trade-secret protection. As PwC explained, “In effect, the Framework may become the de facto standard for cybersecurity and privacy regulation and may impact legal definitions and enforcement guidelines for cybersecurity moving forward.”\textsuperscript{44}

Trade secrets protection is not, of course, only a cybersecurity issue. As a legal matter, the employee agreements, supplier and third-party contracts, and other non-disclosure commitments that a company has in place
are among the most common types of protection that courts look to in determining “reasonable efforts.” Markings and other indications that materials are confidential are also vital steps. Other physical security measures—such as restricted access to company premises, materials and files; segregation of sensitive items in particular locked areas; “clean desk” policies; and requirements to shred sensitive documents—all have been considered by courts as evidence of “reasonable steps.”45

Finally, it is important in designing and implementing any cybersecurity and trade-secrets protections to do an initial and ongoing risk assessment to understand exactly what a company's trade secrets “crown jewels” actually are, and which risks and risk actors are likely to cause the theft or loss of that information. The most technically superior cybersecurity protections done in a vacuum can miss vital, needed protections for trade secrets, if the nature and risks associated with the company's own “crown jewels” are not well defined, and the company's overall cybersecurity and broader trade-secrets protections are not implemented on the basis of rigorous assessment of the risks to those particular “crown jewels.” In many cases, a trade secret inventory and risk assessment can be the most important first steps toward implementing “reasonable steps” that are actually effective in protecting those trade secrets.46

<table>
<thead>
<tr>
<th>TABLE 1. OVERVIEW OF NIST FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FUNCTION</strong></td>
</tr>
<tr>
<td>IDENTIFY (ID)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>PROTECT (PR)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>DETECT (DE)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>RESPOND (RS)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>RECOVER (RC)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
CONCLUSION

Trade secret protection is becoming more and more an issue of cybersecurity. As hackings and other intentional and negligent takings and losses of proprietary information become more commonplace, the legal protections that courts are willing to give a company’s confidential information increasingly will depend on the cybersecurity protections that the company has put in place. The NIST Cybersecurity Framework is proving a popular way of evaluating and managing cybersecurity risks, including risks to trade secrets, and may become a de facto standard for how agencies and even courts evaluate the adequacy of companies’ cybersecurity efforts.

Cybersecurity protections, while vital, are not themselves the “silver bullet” for protecting trade secrets, but run alongside needed contractual protections, physical security, and other trade-secrets specific activities that courts have denominated “reasonable steps.” All of these can be most effectively developed and implemented on the basis of good enterprise risk management practices—understanding what a company’s “crown jewels” are and taking “reasonable steps” to protect them in a well-informed way based on robust risk assessment. This approach to cybersecurity and trade secrets protection not only could help companies to win trade-secrets cases where theft or loss has occurred, but will also help to protect trade secrets more effectively from being misappropriated in the first place.
REFERENCES


4 IBM, supra note 1.


19 Id., art. 2(1).

20 CREATe.org, supra note 17, at 4.


District Court, 46th Civil Division (2005) (no indication on computer list was secret, no password protection, no prohibition on printing and copying – secrecy element not met), http://www.database.iip.or.jp/cases/files/2004%28Wa%2918865.html.


26 Aetna, supra note 24 (“Aetna marks all appropriate documents as confidential and uses technology including password protection and encryption to limit access to confidential information to only key employees.”). See also Complaint, In re Certain Carbon and Alloy Steel Products, supra note 6, at 29 (For confidential directories and files—including the highly sensitive files taken here—U.S. Steel restricts access to employees whose positions require it.).

27 In re Ingle Co., Inc., 116 F.3d 1485 (9th Cir. 1997), http://law.justia.com/cases/federal/appellate-courts/F3/116/1485/612003/ (“Ingle satisfied its burden of showing that it undertook reasonable efforts to protect the secrecy of its research material by presenting evidence that it limited access to research files to Research Department personnel (of which Bauman was not a member), distributed research files only on a need-to-know basis, segregated computer networks, and created limited access research databases.”).

28 United States v. Aleynikov, 2011 U.S. Dist. LEXIS 33345, **3–4 (S.D.N.Y. Mar. 14, 2011), rev’d on other grounds, United States v. Aleynikov, No. 11-1126 (2d Cir. 2012). See also Epic Systems Corporation, supra note 7 (although status of information as trade secrets was effectively undisputed, court noted services agreement provisions that CD drives and USB ports had to be disabled to ensure that TCS employees could not copy data).


32 Aetna, supra note 24; Fortinet Inc., supra note 30; Prime Pay, LLC, supra note 30.


34 United States v. Aleynikov, supra note 28.

35 United States v. Aleynikov, id.


42 See the relevance of and specific cases related to these types of “reasonable steps” in CREATE.org, supra note 17, at 6-13.

REFERENCES, CONT.


45 See CREATe.org, supra note 17, at 6-13.

46 See id. at 9-10.
CENTERT FOR RESPONSIBLE ENTERPRISE AND TRADE (CREATE.ORG)

The Center for Responsible Enterprise And Trade (CREATe.org) is a non-governmental organization (NGO) with a mission to promote leading practices in IP and trade secret protection, cybersecurity and anti-corruption.

To achieve this mission, CREATe.org conducts a range of activities – from publishing reports and whitepapers, and contributing its insights to a range of publications and events – designed to provide practical resources to educate organizations about the leading approaches to managing risk and improving governance and compliance.

CREATe.org launched its wholly-owned subsidiary, CREATe Compliance, to work directly with enterprises on the use of the CREATe Leading Practices services. In addition, CREATe Compliance provides advisory services, training and other guidance.

FOR MORE INFORMATION

To learn more, visit www.CREATe.org or email info@CREATe.org

@2016 CREATe.org All Rights Reserved.