ISSA JOURNAL

March 2014
Volume 12 Issue 3

Cybersecurity Protects Your Company's Valuable Trade Secrets

Guidelines for Designing a BYOD Strategy That Succeeds

The Ethics of Indiscriminate Surveillance

Bypassing EMET 4.1

Cybersecurity Protects Your Company's Valuable Trade Secrets

ISSA Celebrating Cybersecurity 30 Driving Our Destiny

Cybersecurity Protects Your Company's Valuable Trade Secrets

By Frederick Scholl – ISSA Senior Member, Middle Tennessee, USA Chapter
and André (AJ) Bahou, Esq. – ISSA member, Middle Tennessee, USA Chapter

Trade secret thefts have been increasing. The authors define a "trade secret," analyze recent trade secrets cases, referencing the state and federal laws that are applicable to such cases, and conclude with a summary of security recommendations.

Abstract

There are many articles and standards that provide advice and requirements on how to protect personally identifiable information (PII) and how to meet applicable legal requirements. At the same time, trade secret thefts have been increasing and have received significant publicity in matters such as *U.S. v. Aleynikov* and *U.S. v. Nosal*. A number of these cases involve information security operations and policies. This article first defines a "trade secret." Then we analyze trade secrets cases that have made recent news and reference the state and federal laws that are applicable to such cases. We conclude with a summary of security recommendations suggested by both the cases and laws to (1) avoid losing trade secrets to your competitors, and (2) to support legally defensible security if trade secret theft occurs.

Trade secret theft is one of the major cybersecurity risks of our time.[1] Organizations now lose nearly $300 billion per year due to theft or misappropriation of intellectual property.[2] Compare this value with the total 2013 US exports to the EU of $241B. In 1997 the FBI estimated losses to be in the range of $24 billion – $100 billion.[3] Organizations being attacked and making news recently include Nortel, Goldman Sachs, RSA, Lockheed, AMSC, Coca-Cola, QinetiQ, NSA, and many other government agencies.[4] In response to these trends, the administration published its "Strategy on Mitigating the Theft of US Trade Secrets" in February 2013. Today many security managers are focused on preventing the theft of PII (personally identifiable information). In that regard, privacy breaches get broad news coverage and are subject to numerous regulations (HIPAA, PCI, GLBA, etc.). However, there are no regulations stating that you must protect your company's trade secrets.

To protect your trade secrets, your organization must engage in diligent security practices[5] to prevent improper disclosure of your confidential information and proprietary technology.

[1] The Leaky Corporation, *The Economist*, February 24, 2011; The Great Brain Robbery, *Business Week*, March 14, 2012.

[2] The IP Commission Report, May 2013.

[3] *Corporate Espionage*, Ira Winkler, 1997.

[4] "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," February 4, 2014.

[5] "The Legal Defensibility Era," *ISSA Journal*, May 2010.

There are two parts to this effort. First is understanding the legal definition of a trade secret and how courts have handled trade secret theft. Second, one should proactively secure digital assets. Together, these steps will give you a better chance to prevail in court, if you end up in litigation. In the rest of this article, we look at recent trade secret theft incidents, then discuss the laws protecting firms in these matters, and finally the security controls that you must implement to effectively protect your trade secrets.

Although many factors may guide a company to decide whether to seek patent protection on proprietary technology—as compared to maintaining that information in secret—this article will focus on the need for proper security policies and procedures to maintain trade secrets in light of selected recent cases.

Trade secrets defined

A trade secret is a unique form of intellectual property (IP). It can take the form of business documents, databases, SCADA (Supervisory Control and Data Acquisition) control system settings, or other protected know-how. It is one intangible that can potentially last forever—as long as the trade secret is kept secret.

A trade secret (1) is information that has commercial value, (2) is not easily ascertainable by others through proper means, and (3) is subject to reasonable efforts to maintain that information in confidence or secrecy. Albeit much longer, the formal definition of a trade secret in the Uniform Trade Secrets Act (UTSA) is "information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
>
> —*Uniform Trade Secrets Act with 1985 Amendments, §1(4).*[6]

Cybercriminals who attempt to improperly gain access to target company trade secrets are "misappropriating" the trade secrets. Likewise, employees or members of organizations who exceed their authorized access may be liable for misappropriating trade secrets. The technical definition of misappropriation is long and involved,[7] but is generally the acquisition of trade secrets by improper means, misusing the trade secret, or improperly disclosing the information in violation of an obligation to keep the information secret.

Laws governing trade secret theft

Trade secret cases have virtually doubled in the past two decades and are expected to double again by 2017.[8] There are a number of state and federal laws that protect trade secrets. The state laws are modifications of the UTSA. They provide the means for company A to recover any losses resulting from company B's theft of trade secrets, through civil suit. Examples of current and past trade secret state law cases can be found at the Trade Secret Institute website.[9] However, the federal government also protects trade secrets as part of its obligation to secure commerce and to put more teeth in the protection of trade secrets. This federal protection provides criminal prosecution of offenders. Some example federal laws that protect trade secrets include the Economic Espionage Act, 18 U.S.C. § 1832 (EEA) and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (CFAA). The CFAA also provides a way for companies to recover damages (in addition to state law provisions) under its civil litigation provisions. Example CFAA civil cases include *Shurgard Storage Centers v. Safeguard Self Storage*[10] and *E.F. Cultural Travel v. Explorica.*[11]

There are no regulations stating that you must protect your company's trade secrets.

Recent high-profile trade secret cases

While many security incidents go unreported or superficially reported, those cases that result in litigation provide a "gold mine" of information to help understand hackers or malicious insiders. Three recent federal cases involving trade secret theft that we will analyze here are *U.S. v. Nosal*, *U.S. v. Aleynikov*, and *U.S. v. Howley and Roberts*. The first matter involved theft of database records; the second involved alleged theft of software; the third involved theft of tire manufacturing know-how. In all three matters, the US Attorneys got involved and pursued the defendants in criminal litigation. As we mentioned, companies frequently sue the wrongdoers in civil litigation as well.

United States v. Nosal

Mr. David Nosal previously worked for the Korn/Ferry executive search firm.[12] After Mr. Nosal left Korn/Ferry, he enlisted some of his former colleagues that still worked at Korn/Ferry to start a competing executive search business. Those Korn/Ferry employees used their login credentials to gain access to Korn/Ferry's confidential database, including source lists, names, and contact information for potential candidates and companies. A key item to note: those Korn/Ferry employees were authorized to access that information in the

[6] Uniform Trade Secrets Act with 1985 Amendments, §1(2), available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[7] Ibid.

[8] David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293 (2010), http://works.bepress.com/david_almeling/1/.

[9] Trade Secret Institute – http://tsi.brooklaw.edu.

[10] *Shurgard v. Safeguard (*U.S. District Court WD Washington, 2000).

[11] *E.F. Cultural v. Explorica* (First Circuit, 2001).

[12] All citations to *U.S. v. Nosal,* 676 F.3d 854, 856, 858, 863 (9th Cir. 2012) unless otherwise noted.

confidential database. However, Korn/Ferry's policies forbid employees from disclosing that confidential information to Mr. Nosal, who was no longer employed at Korn/Ferry.

The US government indicted Mr. Nosal on twenty counts, which included trade secret theft, violations of the CFAA, and other counts. The government alleged that Mr. Nosal violated 18 U.S.C §1030(a)(4) for aiding the Korn/Ferry employees in exceeding their authorized access with the intent to defraud. In an attempt to win the legal argument, the government argued that the Korn/Ferry employees violated the company "use" policy when they "exceeded authorized access" (under the CFAA) because, although the employees were entitled to access the information, the employees were not permitted to disclose the confidential information to Mr. Nosal. The government therefore argued that the disclosure of that confidential database information was improper because it "exceeded authorized access." The Ninth Circuit Court of Appeals disagreed.

The courts that recognize the proper view of the CFAA prohibit the unauthorized procurement of information but do not criminalize the misuse or misappropriation of trade secrets by employees who may have authority to access that trade secret information but nonetheless violate a company's use policy.

As the Court points out, computers are an indispensable part of our daily work and personal lives. Frequently employees use company-owned computers for personal reasons, and likewise employees use personal mobile devices for company purposes. To aid in management of the company's information, policies are implemented to protect the company's trade secrets and proprietary information. The Ninth Circuit was presented with the legal question whether an employee who violates a company use policy by using a company computer to access confidential databases—does that employee commit a federal crime under the Computer Fraud and Abuse Act, 18 U.S.C. §1030(a)(4)? In short, the Ninth Circuit held that the CFAA does not extend criminal liability to one who "exceeds authorized access" in regards to use restrictions which are defined by the company policies.

The purpose of the CFAA was to criminalize hackers who gain improper access to another's computer system. The Ninth Circuit recognized that if the CFAA were extended to private company's computer use policies—which are seldom read and often vague—then millions of people would be criminals because they watch ESPN, post on Facebook, or view the weather at work on company computers. Those non-business uses of the company computers often violate company use policies but are frequently overlooked. The Court wanted to draw the limits and not make the misappropriation of a company's trade secret database information a crime where that information was properly accessed but not permitted for use by a competitor.

The Nosal case is instructive because it draws a limit around that specific section of the CFAA and does not extend criminal liability under that CFAA to violations of company use policies in that jurisdiction. The Ninth Circuit notes, however, that other Federal Circuit Courts have interpreted the CFAA more broadly to cover violations of organization's computer use policies.[13] The courts that recognize the proper view of the CFAA prohibit the unauthorized procurement of information but do not criminalize the misuse or misappropriation of trade secrets by employees who may have authority to access that trade secret information but nonetheless violate a company's use policy. Moreover, the Ninth Circuit's ruling on the CFAA did not affect the government's charges for theft of trade secrets under the Economic Espionage Act. By way of subsequent activity since the Ninth Circuit's opinion, the FBI announced on its website that Mr. Nosal was convicted on separate criminal charges in 2013, including other trade secret violations.[14]

Goldman and Aleynikov cases

Mr. Sergey Aleynikov was a vice president at Goldman Sachs from May 2007 to June 2009, managing the group that developed source code for Goldman's proprietary high-frequency trading (HFT) system.[15] As a computer programmer, Mr. Aleynikov developed code and algorithms for Goldman's HFT system. Goldman's confidential policies required Mr. Aleynikov to keep the software and proprietary information in strict confidence. Further, those same policies restricted Mr. Aleynikov from taking any of the trade secrets or intellectual property he created with him or using that information when his employment ended with Goldman.

In April 2009, Mr. Aleynikov accepted an offer with Teza Technologies LLC to become its executive vice president for a salary of over $1 million per year, which was more than three times his salary at Goldman. Mr. Aleynikov's role at Teza was to develop a high-frequency trading system for Teza within six months of arriving at his new organization. Normally it would take a team of programmer's years to develop at high-frequency trading system from scratch.

Before leaving Goldman in June 2009, Mr. Aleynikov encrypted and uploaded more than 500,000 lines of Goldman's HFT source code to a server in Germany. When Mr. Aleynikov returned home, he downloaded the source code from the server and placed that source code on a laptop and flash drives. In July 2009, Mr. Aleynikov flew to Chicago to

[13] *U.S. v. Nosal,* 676 F.3d 854, 862 (9th Cir. 2012) ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty.") (citing *United States v. Rodriguez,* 628 F.3d 1258 (11th Cir.2010); *United States v. John,* 597 F.3d 263 (5th Cir.2010); *Int'l Airport Ctrs., LLC v. Citrin,* 440 F.3d 418 (7th Cir.2006)).

[14] FBI Press Release available at http://www.fbi.gov/sanfrancisco/press-releases/2013/executive-recruiter-david-nosal-convicted-of-computer-intrusion-and-trade-secret-charges. (accessed Jan. 25, 2014).

[15] All citations to *U.S. v. Aleynikov*, 676 F.3d 71, 73, 74-75 (2nd Cir. 2012) unless otherwise noted.

meet with his new employer at Teza. He brought the laptop and flash drives to Chicago. Upon returning home to New Jersey, the FBI arrested Mr. Aleynikov at Newark International Airport.

The government charged Mr. Aleynikov with stealing trade secrets under the Economic Espionage Act (EEA) 18 U.S.C. 1832(a) with the intent to convert such trade secrets for the benefit of persons other than its owner Goldman Sachs. The government also charged Mr. Aleynikov with violating the National Stolen Property Act (NSPA) under section 18 U.S.C. 2314 and with unauthorized computer access and exceeding authorized access in violation of the CFAA section 18 U.S.C. 1030. The district court dismissed the count regarding the CFAA because Mr. Aleynikov was authorized to access the source code while he was employed at Goldman. Hence, the CFAA will not be addressed regarding Mr. Aleynikov's case because that count was dismissed, and the count regarding the NSPA will not be addressed for the sake of brevity.

In the Aleynikov case, the Second Circuit overturned a district court's conviction of Mr. Aleynikov based in part on the improper application of the Economic Espionage Act of 1996, 18 U.S.C. 1832. The Second Circuit held that the Goldman source code that Mr. Aleynikov took was not a product "produced for or placed in interstate or foreign commerce" under that statute. Therefore, Mr. Aleynikov's actions did not violate the EEA.

The Second Circuit stated that the source code was not "produced for" or "placed in" interstate or foreign commerce. Rather, Goldman gained significant value from keeping the source code and the HFT system as a trade secret. Because the Goldman high-frequency trading system source code was not placed in commerce, Mr. Aleynikov's theft of the source code was not in violation of the EEA. Similarly, the Goldman HFT system source code was not produced for interstate or foreign commerce because Goldman had no intention of selling its HFT system or licensing it to anyone.[16] Mr. Aleynikov's conduct was in breach of his confidentiality obligations to Goldman, and his dishonest actions should result in civil liability but not criminal liability under the EEA. In regards to the civil liability, there are subsequent civil actions pending between Goldman and Mr. Aleynikov.[17] In those actions, various state trade secret violations are alleged under state law for civil violations of those statutes. In addition, New York authorities arrested Mr. Aleynikov on August 2, 2012, for theft of computer code based on the same actions that were previously considered under the federal EEA.[18]

[16] It is interesting to note that the Second Circuit came to a different conclusion in the *U.S. v. Agrawal* case because the government alleged that the product in that suit was the publicly traded securities that were sold. *U.S. v. Agrawal*, (2nd Cir. Aug. 1, 2013) slip. op. at 13, 23, 51.

[17] *See, e.g., Aleynikov v. Goldman Sachs Group, Inc.*, (D.N.J.) CA No. 12-5994 (KM) (Order on Motion to Dismiss dated Oct. 29, 2013).

[18] Ibid. at 4.

Goodyear case

The Goodyear case[19] is an example of an outsider attack resulting in the theft of trade secrets. While there are many such incidents discussed in the popular press, few result in prosecutions or exact analysis of what happened. This case involves Goodyear, Goodyear equipment vendor Wyko, Wyko engineers Clark Roberts and Sean Howley, and Goodyear competitor HaoHua. The facts are as follows: Goodyear manufactures tires for large earth-moving equipment at its Topeka, Kansas, plant. Wyko is a supplier of tire manufacturing equipment to Goodyear, but not equipment needed to build very large tires. HaoHua had contracted with Wyko to build just this type of equipment, but Wyko did not have the know-how to do so.

In order to prevail and recover in a trade secret case, the injured party must demonstrate that the misappropriated information has financial value.

In response to a routine and unrelated equipment service request by Goodyear to Wyko, Wyko sent two of the engineers involved with the HaoHua project (Roberts and Howley) to the Topeka factory. They took pictures of the Goodyear large tire manufacturing equipment and emailed back to Wyko engineers working on the HaoHua project. In this case, the email was flagged by an internal Wyko IT manager and sent back to Goodyear. Mr. Roberts and Mr. Howley were subsequently convicted of trade secret theft; the decision was upheld by the Sixth Circuit in February, 2013.

Best practices to protect your company's secrets

Protecting trade secrets has both differences and similarities to protecting PII. In this section we will look at controls that may be different for trade secrets protection as well as controls that will overlap with protection of personally identifiable information. PII protection is highly compliance driven. In fact, many security programs are driven overall by PII compliance considerations. Not so for trade secret protection. Additionally, it is relatively easy to identify PII; think HIPAA or PCI, for example. Trade secrets may be in many different formats and stored as structured or unstructured data. Finally, traditional information security analysis often analyzes threats as "insider" and "outsider" threats.[20] In analyzing trade secret risks, another approach is more useful: risks from people you know, and people you don't know. Like murder cases, most trade secret theft involves people you do

[19] *U.S. v. Howley and Roberts*, (Sixth Circuit 2013).

[20] Brian Contos, *Enemy at the Water Cooler*, 2006; Dawn Cappelli, et al, *CERT Guide to Insider Threats*, 2012.

know. They may be employees, contractors, suppliers, or subcontractors to suppliers.

In the cases we described earlier, the perpetrator was apprehended and the secrets recovered; criminal prosecution in two of the three cases was successful as of this writing. The third is still in litigation. However, in many trade secret matters, the injured party fails to recover in court. Edward Roche has summarized four common reasons for this, and we here analyze what security managers can do to avoid this outcome. [21]

Failure to value assets

In order to prevail and recover in a trade secret case, the injured party must demonstrate that the misappropriated information has financial value. It is common for businesses to value their personally identified information, because there are readily available statistics on per-record costs of a breach. However, trade secrets may be found across the organization and, in many cases, no valuation of the information has been carried out. In the Goodyear case, no financial penalties have been levied as yet because of lack of clear financial damage analysis. This is one of the first steps in risk analysis: valuation of assets. For trade secrets it has to be carried out in close collaboration with business process owners. The asset value and probability of loss then provides input to determine the security controls needed.

Failure to classify information

For PII, classification is carried out using data discovery tools and is based on common compliance regimes such as HIPAA or PCI. For trade secrets, the process is more challenging. On the other hand, if not done, then no suitable handling controls can be assigned and the likelihood of protecting the information or defending in a court case is reduced. A critical part of this includes training employees so they will recognize trade secrets. In the Goodyear case, the IT manager did successfully recognize that the photo of the Goodyear equipment was not Wyko's property. Today content-aware, automated DLP tools are available to not only block data exfiltration but automatically classify data. If such DLP tools had been implemented at Goldman, it is possible that code uploads may have been detected earlier.

Failure to earmark trade secrets

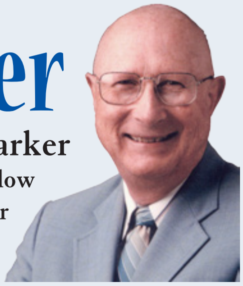
If you do not know what was taken and by whom, and have this documented, you will not have a good defense in a trade secret case. Access logging needs to be activated and logs stored for a reasonable period, depending on the sensitivity and economic value of the secret.

No coordination

If an incident occurs or is suspected, you need to have a response plan in place. This plan should include information security, inside and outside legal counsel, human resources, public relations, information technology, marketing, out-

[21] Edward Roche, *Corporate Spy*, 2007.

Donn's Corner



By Donn Parker
ISSA Distinguished Fellow
Silicon Valley, USA Chapter

Cybercrime

In the last *ISSA Journal* I introduced myself and explained that I will present information security maxims that I have used as terse general truths.

Maxim # 1:

1. We are in the golden age of cybercrime between disaster and annihilation.

Here is maxim # 2:

2. Computers and devices using computers play just four roles in crime: Object, subject, tool, and symbol.

This leads to a general definition of cybercrime in maxim # 3:

3. A cybercrime is an abuse or misuse where a computer or device containing a computer is the object, subject, tool, or symbol, and the perpetrator intentionally made or could have made gain.

First, the computer or device using a computer may be the object of the crime as a target to do physical, electrical, or logical harm to it. I have found cases where revenge-bent perpetrators destroyed or damaged computers and attacked devices by every means imaginable. This leads to another maxim:

4. Fragile computers as objects of great importance have been shot, blown up, kicked, shaken, drowned, electrocuted, fried, baked, burned, urinated upon, dropped, stolen, held for ransom, lost, irradiated, and sat on.

Next, computers may play the role of subject in a cybercrime by forming unique environments in which perpetrators engage or threaten to engage in abuse and misuse. This includes introduction and execution of malware, Trojan horse attacks, buffer overflow attacks, denial of service, and deceptions.

Third, perpetrators may use computers or devices using computers as tools to perpetrate abuse and misuse much as burglars might use a crow bar. A cipher expert might use a computer as a tool to break an encrypted message from another computer. A violent perpetrator could use a computer as a murder weapon by hitting somebody on the head with it or by using the computer that controls a medical instrument.

Finally, there is one often overlooked role of computers. A fraudster may or may not use a computer at all but refer to it as the symbol, image, or evidence of use of a powerful, trustworthy, and presumably fact-producing computer. This role of a computer would be to intimidate, impress, comfort, or deceive victims. It attaches a legitimacy, capability, and significance to a fraudulent activity for a supposed victim's benefit such as investing in shady enterprises. This leads to another maxim:

5. If it came from a computer, it must surely be correct, true, and significant.

I have found all four and many combinations of the roles of computers among cybercrimes documented in my files. Can you think of any other role of a computer in cybercrimes?

Donn Parker, CISSP, Retired, Distinguished Fellow, and information security pioneer, donnlorna@aol.com.

sourcing firms, law enforcement, and C-suite members if necessary. The plan should be practiced at least semi-annually with varied scenarios. Software tools are now available to support the planning process as well as the operational steps during an incident. The incident response plan should be developed in cooperation with data recovery/business continuity planning leaders.

Other steps should be taken to prevent misappropriation and to further improve courtroom defense, if needed.

Minimize legal vulnerabilities

To start with, an overall defensibility strategy should be developed in collaboration with your organization's general counsel.[22] Well written and up-to-date non-disclosure agreements (NDA) are mandatory for all employees, contractors, and suppliers. A well thought out termination policy is also mandatory. Such a policy should include a risk analysis of the departing employee. A better policy may have prevented the Korn/Ferry breach incident discussed above. Background checks are now routine and part of onboarding for employees and contractors. However, recent news articles have questioned the accuracy of such checks.[23] It may be that background check firms have worked to reduce false positives and have thus enabled more false negatives than would be desirable. Validating the accuracy of your background checks may reduce the risk of future employee or contractor issues.

Manage outsourcing risks

Outsourcing, both traditional and cloud based, continues unabated. A broad range of risks exists here from the supplier reputation to the location of your data. Your supplier countries may not have adequate IP protection for your firm's trade secrets. Country-by-country assessments are available from the Office of the United States Trade Representative.[24] Nonetheless, many firms are doing business in high-risk countries and security managers will need to mitigate these risks. A good reference guide for this process is ISO 27036, "Guidelines for Security in Outsourcing."[25]

Harden the data

This is an approach that is common with PII security environments. Defense in depth has been the usual approach. The problem is that each layer has one or more gaps, and smart actors have learned how to navigate their way through to access sensitive information. Operational management of these architectures has also been a big challenge. Today's solution is all-in-one "data firewalls" that include all essential features, including firewall, encryption engine, and key management and logging; the benefit is ease of installation and management.

Conclusions

Security managers are going to continue to be challenged by changing technology and globalization. New exfiltration paths for trade secrets have been created: cloud,[26] social media,[27] BYOD, and APT.[28] These paths will continue to be monetized in new ways by threat actors. A critical common factor is response time. The cadence of security programs must be improved beyond the annual audit response time to respond to more rapidly changing threats. This includes better and more rapid threat intelligence, threat response, and incident response. Threat intelligence and incident response can be improved using automated tools and services. Better threat response is determined by the effectiveness of the security program in communicating risk to the C-suite.[29] Developing a strong trade secret protection program in support of your business is a good opportunity to work with business leaders and improve overall communication and support of your security program.

The views expressed herein are solely the authors' opinions and do not necessarily reflect the opinions of their company or organization. This article is not intended to render legal advice. If you seek legal advice, please consult an attorney in your jurisdiction for applicable laws specific to your situation.

About the Authors

Frederick Scholl, PhD, CISSP, is president of Monarch Information Networks, LLC and Visiting Professor of Information Security at Lipscomb University. He may be reached at freds@monarch-info.com.

André (AJ) Bahou, Esq., serves as corporate counsel, vice president and chief intellectual property officer for Prism Technologies, LLC. Mr. Bahou practices in the area of intellectual property law, including litigation management of patents, copyrights, trademarks, and trade secrets. He focuses in the technical areas of computer hardware, software, and networking security for the Internet and mobile telecommunications. Mr. Bahou has an LLM in Intellectual Property Law and is currently vice president of the Tennessee Intellectual Property Law Association. He may be reached at aj.bahou@prsmip.com.

[22] The Legal Defensibility Era, *ISSA Journal*, May 2010.

[23] Contractors will no longer review their own background checks, *Washington Post*, February 7, 2014.

[24] Office of the United States Trade Representative – http://www.ustr.gov.

[25] ISO/IEC 27036-1, Information Security for supplier relationships-Part 1: Overview and concepts, about to be published.

[26] "Trade Secret Spat Centers on the Cloud," www.therecorder.com, Sept. 20, 2013.

[27] "Goldman Looks to Ban Some Chat Services Used by Traders," online.wsj.com, January 23, 2014.

[28] *Advanced Persistent Threa*t, Eric Cole, 2013.

[29] Target Staff Had Warnings, *Wall Street Journal*, February 15-16, 2014.