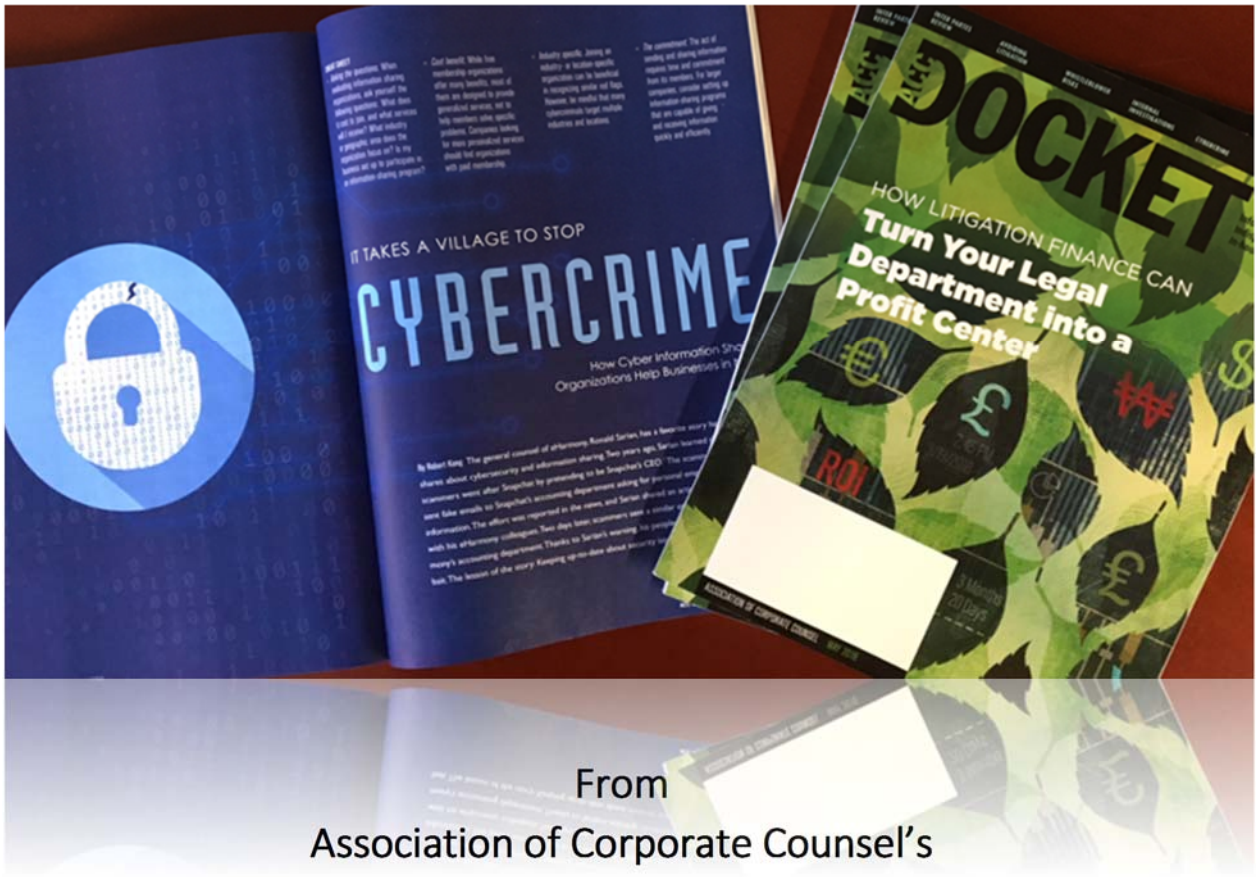
It Takes a Village to Stop Cybercrime

How Information Sharing Organizations
Help Businesses in Need

Robert Kang
Adjunct Professor, Loyola Law School
kangr@lls.edu



From
Association of Corporate Counsel's
ACC Docket
May 2018
www.ACC.com

CHEAT SHEET

- *Asking the questions.* When evaluating information sharing organizations, ask yourself the following questions: What does it cost to join, and what services will I receive? What industry or geographic area does the organization focus on? Is my business set up to participate in an information-sharing program?
- *Cost benefit.* While free membership organizations offer many benefits, most of them are designed to provide generalized services, not to help members solve specific problems. Companies looking for more personalized services should find organizations with paid membership.
- *Industry specific.* Joining an industry- or location-specific organization can be beneficial in recognizing similar red flags. However, be mindful that many cybercriminals target multiple industries and locations.
- *The commitment.* The act of sending and sharing information requires time and commitment from its members. For larger companies, consider setting up information-sharing programs that are capable of giving and receiving information quickly and efficiently.

IT TAKES A VILLAGE TO STOP CYBERCRIME

How Cyber Information Sharing Organizations Help Businesses in Need

By Robert Kang The general counsel of eHarmony, Ronald Sarian, has a favorite story he shares about cybersecurity and information sharing. Two years ago, Sarian learned that scammers went after Snapchat by pretending to be Snapchat's CEO.[1] The scammers sent fake emails to Snapchat's accounting department asking for personal employee information. The effort was reported in the news, and Sarian shared an article about it with his eHarmony colleagues. Two days later, scammers sent a similar email to eHarmony's accounting department. Thanks to Sarian's warning, his people didn't take the bait. The lesson of the story: Keeping up-to-date about security issues pays off.[2]

The sharing organization anonymizes (if requested), aggregates, and processes the submissions and, in some cases, enriches it with nonpublic information provided by government agencies or other sources. The sharing organization then returns the processed information to its members as reports, aggregated lists of suspicious IP addresses, and more.

Sarian is the first to acknowledge that his story contained an element of luck. To minimize the need for luck, governments and various industries have created organizations designed to share security-related information among their members in a structured, regular manner. Often called "public/private partnerships" and "information sharing organizations," many of them follow a similar model: They are organized as nonprofit entities, and their members send information, like suspicious IP addresses and other threat indicators, to them. The sharing organization anonymizes (if requested), aggregates, and processes the submissions and, in some cases, enriches it with nonpublic information provided by government agencies or other sources. The sharing organization then returns the processed information to its members as reports, aggregated lists of suspicious IP addresses, and more. Some organizations also provide security training and other services.

"Sounds good," a hypothetical CEO, chief information security officer, or GC may think, "Let's join some info sharing organizations." But where to start? Look up "cybersecurity information sharing organization" on the internet and be ready to face a bewildering slew of options from "ISAC" to "InfraGard." This article is intended to help business and legal professionals sift through several well-known options and find one that may make the most sense for your business. In evaluating these organizations, ask yourself the following questions:

- What does it cost to join a particular organization, and what services will I receive?
- What industry or geographic area does a particular organization focus on?
- Is my business set up to participate in an information sharing program?

1. Cost versus services provided

The first questions to ask are "what will it cost to join an information sharing organization, and "what services will my business receive in return?" The answers depend on the type of services that you want to get out of joining. For smaller companies with few resources, a good option may be to join organizations that offer free services, like the FBI-associated nonprofit InfraGard. "You'll need to pass an FBI background check to join," said Gary Gardner, the chairperson of its national board of directors. "But once you do, you'll have access to many things, including unclassified FBI reports and the ability to take free training courses nationwide." Gardner further explained that InfraGard is a volunteer-driven organization with local and regional chapters. Members have even formed special interest groups focusing on specific issues, like legal services and business continuity. And while small companies may benefit from joining, it's telling that over 400 of the nation's Fortune 500 companies have InfraGard representatives.

While free membership organizations offer many benefits, most of them are designed to provide generalized services, not to help members solve specific problems. Companies seeking more sophisticated, personalized services should look to organizations with paid membership requirements.

Robert Kang is an adjunct professor for cybersecurity and technology at Loyola Law School, Los Angeles, where he helped design and launch the first comprehensive cybersecurity and data privacy law concentration on the West Coast. He is also a senior counsel at a Fortune 500 company. As the former co-chairperson for the Los Angeles chapter of the International Association of Privacy Professionals, Kang organized cybersecurity, data privacy, and risk management programming for the public. He speaks regularly on the subject. *kangr@lls.edu*

A walkthrough of several information sharing organizations

GLOBAL RESILIENCE FEDERATION

Launched in 2017, the federation is an alliance of ISACs and ISAOs wishing to coordinate information sharing among them. The federation is a nonprofit entity, and its leaders have played key roles in launching and managing the Financial Services ISAC and the Legal Services ISAO. The federation shares information among these organizations to collaboratively identify and fight common threats. The federation can also help industries create their own ISACs/ISAOs.

Who are potential members? The federation is made up of selected ISACs and ISAOs. Businesses join by joining organizations that belong to the federation.

- For more information, visit *www.grfederation.org.*

INFRAGARD

The FBI describes InfraGard best: It's a nonprofit association of persons who represent businesses, academic institutions, state, and local law enforcement agencies and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.[6] Members report suspicious activity to InfraGard and receive access to unclassified reports, including those provided by government agencies, about cybersecurity and physical security. InfraGard also features regional chapters and member-organized special interest groups focusing on specific issues. Finally, InfraGard offers free training courses throughout the United States.[7] InfraGard, however, is designed to provide general, not personalized, services. There is no fee to join, but failure to participate regularly may forfeit your membership.

Who are potential members? Membership is open to US citizens. You'll need to fill out an application explaining why you want to join, and pass an abbreviated FBI background check. Over four hundred of the nation's Fortune 500 companies have InfraGard representatives.

- For more information, visit *www.infragard.org.*

ISACS AND ISAOS

For most practical purposes, ISACs and ISAOs are the same thing: nonprofit information sharing organizations focused on serving specific industries or geographic locations. The primary difference is that ISACs support certain "critical infrastructure" industry sectors such as energy and water. In contrast, ISAOs serve other industries such as the sports industry. These organizations charge membership fees, but they provide personalized services in return. Think of them as de facto trade organizations.

Who are potential members? Because there are membership fees involved, membership may be best for businesses that achieve a requisite level of size, success, and sophistication and thus require an equivalent level of sophisticated information sharing services.

- For more information about ISACs, visit *www.nationalisacs.org.*
- For more information about ISAOs, visit *www.isao.org/information-sharing-groups.*

NCFTA

A nonprofit organization launched with support from the FBI, the NCFTA is a well-established cross-sector, cross-locational information sharing program.[8] NCFTA members have access to unclassified reports about cybersecurity, physical security, and even brand and content protection services. Members also have access to a malware lab and a team of over 40 trained security analysts capable of assisting businesses on individual matters. FBI and other government agents are assigned to assist NCFTA. By aggregating an individual member's security concerns with information provided by other members, NCFTA has assisted its members to develop criminal cases that have attracted law enforcement involvement. There are membership dues.

Who are potential members? The same types of companies seeking to join an ISAC or ISAO. However, look to NCFTA to send and receive information across multiple industries and locations.

- For more information, visit *www.NCFTA.net.*

"For example," said Matthew LaVigna, CEO of the National Cyber Forensics & Training Alliance (NCFTA), "our organization is staffed with over 40 intelligence and security analysts."

LaVigna explained that NCFTA membership opens up access to many services, including access to those analysts. "Shoot us a question, and our people will take [that question] and run with it," he said. If the issue is sufficiently serious, NCFTA helps the company build a criminal case to attract law enforcement attention. NCFTA members also have access to

Cybersecurity and privacy certifications: Finding the right one

As one of the earliest generation of in-house cybersecurity counsel, I did my cybersecurity and data privacy training on the job. But there are many programs that offer robust formal training and certifications for in-house counsel that want to learn about the industry. Choosing the right one for you requires balancing the following: cost, study time, and the value offered by the certification.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS "CIPP" CERTIFICATION

Job hunters looking for "privacy counsel" positions will begin seeing a common set of preferred qualifications: "IAPP certification preferred" or "CIPP preferred." The former refers to the International Association of Privacy Professionals, and the latter refers to that organization's Certified Information Privacy Professional certification. This certification is turning into one of the most commonly recognized privacy certifications for attorneys.

IAPP offers several flavors of CIPP certification: CIPP/US denotes knowledge of US privacy laws; CIPP/E denotes knowledge of European privacy laws, and so on. There are management and technical certifications, too. The CIPP certification may be useful to in-house counsel who perform privacy-related legal and regulatory functions. It's important to note that the CIPP certification is not, strictly speaking, a cybersecurity certification (i.e., privacy deals with collecting and managing information; cybersecurity deals with stopping bad actors from taking it). But it's not uncommon for cybersecurity attorneys to obtain CIPP certification.

IAPP's upfront costs (both time and money) are on the lower end of the options described here, as IAPP allows for self-study. Successful CIPP test takers report spending about 60 hours of self-study to prepare. IAPP offers tests throughout the United States, and in some international locations, so finding a location is not difficult. However, IAPP membership involves some ongoing costs. IAPP members pay annual dues and must take continuing professional education (CPE) courses similar to CLEs. However, many IAPP-approved educational programs offer combined CLE and CPE credit, which defrays some of that cost. IAPP members also gain access to listservs and other member-only privileges.

- For more information, visit *www.IAPP.org.*

INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM (ISC2) "CISSP" CERTIFICATION

The Certified Information Systems Security Professional (CISSP) is a well-known certification offered by ISC2. The value of this certification for attorneys is real, if narrow, as the CISSP is geared toward IT professionals. The certification process, for example, only lightly touches on legal and regulatory issues. The time commitment for obtaining a CISSP is high: It's not uncommon to hear that CISSP holders spent up to nine months of self-study preparing for the test — possibly more if the test-taker lacks a technical background. Testing locations are available worldwide. The number of attorneys with a CISSP certificate is low compared to IAPP certificate holders. *(continued on the next page)*

A CISSP certification may be useful for in-house counsel who work closely and regularly with IT staff, for example on technical quality assurance matters. It may be less useful for attorneys who focus on legal and regulatory matters. However, the CISSP's rarity amongst attorneys offers one significant benefit: "Getting a CISSP certification gives you credibility with technical professionals," says David Coher, a CISSP holder and member of the advisory board of the Georgetown Cybersecurity Law Institute. "They know the work that went into getting it."

- For more information, visit *www.isc2.org.*

SANS INSTITUTE "GLEG" CERTIFICATION

The SANS Institute offers a certification in the Law of Data Security and Investigations (GLEG). Although online options are available, many students take one of SANS' live five-day courses. The upfront costs (both time and cost) to take a five-day course at SANS will be higher than the self-study options offered by IAPP or ISC2, but SANS training often qualifies for company educational reimbursement programs. Recipients of the GLEG certification must recertify every four years.

SANS training may help counsel whose practices focus on litigation, in addition to privacy and regulatory matters. SANS certification is not well known to many attorneys, but it is prominent in the eyes of dedicated security professionals.

- For more information, visit *www.giac.org.*

LAW SCHOOL JD/LLM PROGRAMS

Some in-house counsel may seek a wide-ranging education in privacy or cybersecurity. If so, a handful of law schools, such as the University of Maryland Francis King Carey School of Law, offer cybersecurity LLMs. Those seeking balmier weather may want to explore Loyola Law School, Los Angeles' LLM program, the first of its kind in the West Coast. Upfront costs to obtain an LLM degree will be higher in terms of time and money than the other options described here, but students earn an LLM in return. Company educational reimbursement programs may help defray costs. This option may be useful for in-house counsel seeking a comprehensive, wide-ranging understanding of cybersecurity and technology. For example, in addition to conventional cybersecurity survey courses, Loyola offers courses in incident response management, digital media, and more.

In-house counsel may also choose to audit individual technology-focused classes from schools like Loyola or from their local law school. Potentially useful courses to take include cybersecurity, data privacy, digital media, and technology transactions.

- For more information, visit your law school's website.

a malware analysis portal and other services beyond those provided by free membership organizations.

2. Joining an industry-specific sharing organization versus a cross-industry organization

The next question to ask is whether to join an organization that focuses on specific industries and geographic locations or not. "ISACs" and "ISAOs" (information sharing and analysis centers and information sharing and analysis organizations, respectively) are the most common type of industry-specific and location-specific cyberinformation sharing organizations (despite the difference in names, ISACs and ISAOs are effectively the same thing). Membership into the Financial Services ISAC, for example, is limited to banks, brokerages, and other financial institutions. Similarly, only law firms are allowed to join the Legal Services ISAO. There's even an ISAO for the sports industry. "ISACs and ISAOs are a combination of information sharing program and trade association," said Cindy Donaldson, the president of the Global Resilience Federation, an information sharing alliance that includes the Financial Services ISAC and Legal Services ISAO. "Our members are in specific industries, and we develop expertise about issues and threats facing those industries to better serve them."

ISAC and ISAO members may also receive government assistance, since these organizations act as natural touch points for government agencies to share industry-specific tools and information with. For example, when the US Department of Energy (DOE) wanted to provide certain grid-focused cybersecurity tools to electric utilities, the DOE didn't contact the utilities individually. Instead, the DOE sought help from the Electricity ISAC. The result is the "Cybersecurity Risk Information Sharing Program" — an innovative program designed to enhance national security, which is run by the industry's ISAC and not by the DOE.[3]

Joining an industry or location-specific sharing organization has many benefits. But it's important to remember that many cybercriminals target multiple industries and ignore geographic boundaries. Thus, many businesses join information sharing organizations with charters that cut across different industries and locations. These organizations look for criminal connections

that may not be visible to security professionals focusing on a single industry sector or locale.

"Look at Global Airline Action Days," said LaVigna, NCFTA's CEO, when asked for examples of multi-industry, multinational cooperation.[4] "It's a program that started with Europol, to identify and arrest suspected airline fraudsters. When the US decided to participate, we [NCFTA] became the US coordinator for the program."

LaVigna explained that NCFTA receives information from credit card companies about suspect purchases and compares those purchases with other information provided by airlines and law enforcement agencies. Correlating that data yielded some surprising connections. "Lots of people think airline fraud is about getting a free airline ticket," said LaVigna. "But put all this [cross-industry] information together and you begin seeing patterns of wider criminal activity." For example, from October 16-20, 2017, law enforcement agents in 61 countries and 226 airports, used information processed by NCFTA and similar organizations to arrest nearly 200 people.[5] In addition to nabbing ticket scammers, the information enabled law enforcement to target and arrest individuals suspected of drug trafficking, human smuggling, and immigration fraud.

The trend for developing cross-industry ties is growing. For example, last year, three industry-specific information-sharing organizations (the Energy Analytic Security Exchange, the Financial Services ISAC, and the Legal Services ISAO) joined forces to form a multi-industry coalition: the Global Resilience Federation. When asked why these organizations banded together, the federation's Donaldson responded, "to handle common threats, including pervasive and dangerous ones that cut across industries, like WannaCry and NotPetya."

3. Determining whether your company is set up to participate in particular information sharing organizations

Information may be shared among organizations in a variety of ways: listservs, automated information sharing systems, online portals, emails, and more. Because participating in any program requires time and resources (to read and act upon emails, if nothing else), the final question to ask yourself is whether your business is up to the task of sending and receiving information effectively. In other words, before joining an organization, you should decide what level of information you're prepared to send and receive.

As noted earlier, smaller businesses with few resources, but with a desire to share, may want to start by joining organizations like InfraGard, which requires little in the way of startup or participation costs. But there is a limit to the information that gets shared. For example, free membership organizations typically share threat information via written reports, which take time to develop. On the other end of the spectrum are paid-membership organizations, which offer a greater array of services but expect an equivalent commitment from members. For example, some paid-membership information sharing organizations offer direct "machine-to-machine" transfer of threat information between them and their member businesses. This type of sharing enables businesses to receive — and act upon — threat information very quickly. But it takes time and money for companies to set up internal programs capable of participating.

The act of sending and sharing information requires time and commitment from its members. Starting small is logical for smaller companies but limited. For larger companies, setting up information sharing programs that are capable of giving and receiving sophisticated levels and types of information may generate real value for their businesses. Finally, sophisticated businesses may consider joining more than one

information sharing organization; think of it as applying a "defense in depth" strategy for information sharing.

Conclusion

In days past, companies may have been reluctant to share information about cybersecurity issues with others. But in today's interconnected society, no single entity can fight the threat of online intrusion alone. It takes a village to protect businesses from cybercrime; joining an information sharing organizations provide the means for businesses to become part of that village. **ACC**

1 GC of eHarmony Ronald Sarian Battles Cyberattacks With Knowledge, Careful Planning (Dec. 2017) *www.law.com/corpcounsel/sites/corpcounsel/2017/12/04/gc-of-eharmony-ronald-sarian-battles-cyberattacks-with-knowledge-careful-planning.*

2 Related: So What Does General Counsel Have to Do with Cyber-Security, Anyway? (2016) *www.legal.cioreview.com/cxoinsight/so-what-does-general-counsel-have-to-do-with-cybersecurity-anyway-nid-13121-cid-65.html*.

3 Letter fromthe United States Department of Energy explaining the Cybersecurity Risk Information Sharing Program (Aug. 2014) *www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20%28CRISP%29.pdf.*

4 EuroPol — About Airline Action Days *www.europol.europa.eu/operations/airline-action-days*.

5 Authorities Catch 200 Plane Ticket Fraudsters (Oct. 2017) *www.travelweekly.com.au/article/authorities-catch-200-ticket-fraudsters.*

6 FBI — About InfraGard *www.fbi.gov/about/partnerships/infragard*.

7 Related: InfraGard Los Angeles Training & Events *www.infragardlosangeles.org/infragard-events.shtml*.

8 The FBI Workaround for Private Companies to Share Information With Law Enforcement Without CISPA (April 2012) *www.forbes.com/sites/kashmirhill/2012/04/26/the-fbi-workaround-for-private-companies-to-share-information-with-law-enforcement-without-cispa/#79c431b65009.*

ACC EXTRAS ON… Cybersecurity

ACC Docket

Yahoo's 10K: Lessons on What Not to Do in a Breach (Nov. 2017). *www.accdocket.com/articles/yahoo-10k-lessons-on-what-not-to-do-in-a-breach.cfm*

How to Reduce Your Cybersecurity Risk Profile through Vendor Management (July/Aug. 2017). *www.accdocket.com/articles/reduce-your-cybersecurity-risk-vendor-management.cfm*

This Week in Privacy: What Is the New IoT Cybersecurity Bill? (July/Aug. 2017). *www.accdocket.com/articles/the-new-iot-cybersecurity-bill.cfm*

InfoPAK

Corporate Crime Multi-Jursidictional InfoPAK (Jan./Feb. 2017). *www.acc.com/legalresources/resource.cfm?show=1451965*

Practical Tools to Implement and Assess a Big Data Program (Sept. 2016). *www.acc.com/legalresources/resource.cfm?show=1438035*

QuickCounsel

When "WannaCry" Strikes: Preparing for and Responding to the Largest Ransomware Attack in History (May 2017). *www.acc.com/legalresources/resource.cfm?show=1459241*

Cybersecurity Failures and Resulting Liability Issues (April 2016). *www.acc.com/legalresources/quickcounsel/cybersecurity.cfm*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.