Secrecy and Privacy

The COVID-19 pandemic has accelerated many trends in information technology that were already evident before the global outbreak, including teleworking, cloud-based hosting and distance learning. Not all the accelerated trends were positive, however. One such has been the focus on secret information by cyberattackers.

> "I SUBMIT THAT THE PROTECTION OF SECRET INFORMATION, OVER AND ABOVE PRIVATE INFORMATION, WILL BE THE NEXT BIG THING FOR CYBERSECURITY."

Clearly, the theft of information is not a new phenomenon, but the most publicized attacks have been those on personal data resulting in breaches of millions of people's privacy. A different sort of data theft has been cyberattacks on trade secrets.[1] I believe that the importance of protecting secrecy in addition to privacy has been heightened at this time.

Information Secrecy Factors in the Pandemic Era

Why now? The foremost factor has been governments attacking other states' industrial secrets.[2, 3, 4] Not unrelated, we are in a period of growing international trade conflicts[5] that are raising the stakes both for preserving and stealing trade secrets. Moreover, the pandemic has caused many countries to erect barriers where none existed before.[6] Additional concerns are the incidence of insiders perpetrating cyberattacks[7] and the eagerness of some Big Tech companies to scoop up all the information they can.[8]

Taken together, these factors pose a newly intensified threat to industrial and governmental secrets and of cyberattacks as a means of getting to them. I submit that the protection of secret information, over and above private information, will be the Next Big Thing for cybersecurity. (Lest my information security brethren and sistren smite me mightily about the temples for apostasy, I am in no way minimizing the problems posed by theft of personal information, ransomware, and other manipulative and destructive attacks. I am just saying that there is a new problem to add to the list.)

Privacy and Secrecy

Clearly, the secrecy and the privacy of information are related. At the most elemental level, both are based on confidentiality,[9] the prevention of dissemination of items of information. Privacy implies the retention of interest by the data *subject* in the information about herself or himself. (Note that privacy refers only to information about people.) Secrecy is a higher level of interest by the data *owner* in limiting knowledge of certain information.

Steven J. Ross, CISA, CDPSE, AFBCI, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

Enjoying this article?

- Read *Privacy: Beyond Compliance. www.isaca.org/privacy_beyond_compliance_2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

There is, obviously, some overlap between the two concepts. Some private information may also be secret, and some secret information may also concern people. For example, espionage agencies' information concerning the identity of their spies falls into both categories, though I imagine that secrecy takes precedence. However, it is not so clear that the controls for privacy work equally well for secrecy. Perhaps a closer examination of the attributes of the two will provide some enlightenment.

The Attributes of Privacy

The American Institute of Certified Public Accountants (AICPA) and what is known today as Chartered Professional Accountants (CPA) Canada have developed a framework known as Generally Accepted Privacy Principles (GAPP).[10] For purposes of this discussion, I offer below a grossly abbreviated list of its 10 principals:

1. **Management**—Definition, documentation, communication and accountability for data
2. **Notice**—Notification of policies, procedures and purposes
3. **Choice and consent**—Availability of choices to the individual, with implicit or explicit consent for collection, use and disclosure
4. **Collection**—Collection of data only for the purposes identified in the notice
5. **Access**—Individuals' access for review and updating of data about themselves
6. **Use, retention and disposal**—Limitation of use to the purposes in the notice with consent; retained only as long as necessary for the purpose and then disposed of
7. **Disclosure to third parties**—Disclosure only for the purposes in the notice and with consent
8. **Security**—Protection of data against unauthorized access
9. **Quality**—Accuracy, completeness and relevance of information
10. **Monitoring and enforcement**—Assurance of compliance with policies and procedures

The Attributes of Secrecy

For this list, I drew upon and expanded definitions offered by the US Patent and Trademark Office:[11]

- **Utilization**—The information must be used for a purpose
- **Advantage**—The information provides benefit to the owner that is denied to those not having it
- **Value**—The information has inherent worth
- **Uniqueness**—The information is not generally known nor can it be derived independently
- **Active security**—The information is protected by means beyond those used for nonsecret information (e.g., classified systems, armed guards)

Commonality of Attributes

It seems to me that certain of these attributes apply only to privacy: management, notice, choice and consent, and access. Uniqueness applies only to secrecy. However, there is significant commonality among the others:

- For reasons that should be self-evident to readers of this *Journal*, security is a common attribute, although it is not mentioned as one for secrecy. Secrets cannot be kept without it.
- "Utilization" is just a five-syllable word for "use," so I see "use, retention and disposal" as being roughly equivalent between privacy and secrecy. Importantly, the manner in which information is stored and disposed of is essential to the purpose for which it was created. The purpose of the information is generally evidenced by its handling. Just as a secret written on paper cannot be left on a desktop, so the electronic equivalent requires secure storage and erasure.
- The way in which information is made available (or not) to third parties is a determinant of the advantage a recipient might have. Put another way, someone whispering, "Don't tell a soul, but Mary is going to be fired," breaches both privacy and secrecy. The same may be said of the electronic version of "sharing" secret information.
- The value of information is inherently tied to its accuracy. If it is Joe who is about to be let go, not Mary, then the whispered gossip is no secret at all.
- All information security, including privacy, requires monitoring. What differentiates secrecy is the extent of enforcement. Secrecy requires the owner of the information to take additional, specific

measures to ensure that security is maintained. If access to all information requires a user ID and a password, then, while those are necessary for secrets, they are insufficient. Something more must be done to protect true secrets.

What to Do About Secrets

To reiterate, whatever security practices are in place for cybersecurity should stay there. Based on the analysis I gave previously, it seems to me that the overlap of secrecy and privacy calls for the extension of an existing privacy program, assuming that an organization has one. If it does not, it ought to, if only to be compliant with laws and regulations.[12]

Then an organization should determine what information it has that is, in fact, secret. Some secrets have enormous and long-lasting secrecy requirements; how to build weapons of mass destruction surely falls into this category. On the other hand, financial information that is due to be publicly released in days is also secret, especially if it might affect stock prices. Considered broadly, almost every organization and government agency has some information that should be closely held. The challenge is to determine what and where it is.

Secrets, as opposed to private information, are unlikely to be found in structured files and databases. The more likely hiding places are in unstructured data, such as file shares, documents (including electronic documents) and in collaboration tools such as Microsoft's SharePoint.

A secrecy program, added to that for privacy, necessitates… Uh-oh, my editor tells me I have run out of room. I will reveal the, *ahem*, secrets in my next article.

> "IT SEEMS TO ME THAT THE OVERLAP OF SECRECY AND PRIVACY CALLS FOR THE EXTENSION OF AN EXISTING PRIVACY PROGRAM, ASSUMING THAT AN ORGANIZATION HAS ONE."

Endnotes

1 A Google search for information regarding cyberthefts of trade secrets resulted in many citations, most of them—in English—from the period since the outbreak of the pandemic and most of them concerning Chinese attacks on American industry. I also tried a Baidu search, which resulted in fewer and less contemporary results. But those in English showed the reversed point of view, denying Chinese attacks. For an earlier and more balanced perspective, see: Villaseno, J.; "Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur," Hoover Institution, August 2015, *https://www.hoover.org/sites/default/files/corporatecybersecurityrealism.pdf*.

2 In the United States, much attention has been given to Chinese incursions on Western pharmaceutical companies' vaccine research. See: Nakashima, E.; D. Barrett; "US Accuses China of Sponsoring Criminal Hackers Targeting Coronavirus Vaccine Research," *The Washington Post*, 21 July 2020, *https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html*.

3 In the United Kingdom, more attention has been focused on attacks from Russia. See: Rayner, G.; "Russian Hackers Attempted to Steal UK's Covid-19 Vaccine Research, Downing St. Says," *The Telegraph*, 17 July 2020, *https://www.telegraph.co.uk/politics/2020/07/16/russian-hackers-attempted-steal-covid-19-vaccine-research-downing/*.

4 Not surprisingly, the Chinese press (or at least the English-language versions) see it differently. See: Wang, Q.; "US Accusations of Vaccine Theft 'Absurd,'" *China Daily*, 18 July 2020, *https://global.chinadaily.com.cn/a/202007/18/WS5f123a07a31083481725a64b.html*.

5 Campbell, C.; "The U.S.-China Trade War Is Steering the World Toward Crisis and There Is No Easy Retreat," *Time*, 17 August 2019, *https://time.com/5645964/donald-trump-china-trade-war-crisis/*

6 Organisation for Economic Co-operation and Development (OECD), "COVID-19 and International Trade: Issues and Actions," France, 12 June 2020, *https://www.oecd.org/coronavirus/policy-responses/covid-19-and-international-trade-issues-and-actions-494da2fa/*

7 Monpetit, J.; "Personal Data of 2.7 Million People Leaked From Desjardins," CBC, 20 June 2019, *https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297* This theft was perpetrated by a disgruntled employee.

8 Zuboff, S.; *The Age of Surveillance Capitalism*, PublicAffairs, USA, 2019

9 Defined by the *Merriam-Webster Dictionary* as "private, secret," which does not do much to clarify the distinction between the terms. So I have given my own definition.

10 Chartered Professional Accountants, Canada, "Generally Accepted Privacy Principles (GAPP) in Privacy Policy Development," 2009, *https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development*

11 United States Patent and Trademark Office, "Trade Secret Policy," USA, 11 May 2016, *https://www.uspto.gov/ip-policy/trade-secret-policy*

12 Not least among those is the EU General Data Protection Regulation (GDPR), which calls for most enterprises to have a data protection officer who can also oversee a secrecy program.

CCAK™

Certificate of Cloud Auditing Knowledge

A Cloud Security Alliance® and ISACA® Credential

Elevate Your Cloud Auditing Expertise with a Vendor Neutral, Technical Credential

Take on the unique challenges of auditing the cloud with the first-ever global cloud auditing credential. Developed by global leaders Cloud Security Alliance® (CSA) and ISACA®, the new **Certificate in Cloud Auditing Knowledge** provides a thorough understanding of:

- Cloud audit terminology, constitution and delivery methods.
- Technology stacks, deployment frameworks, DevOps, CI/CD, automation and governance.
- Transparency, encryption, colocation, scale, etc. in the cloud.

Learn more: **www.isaca.org/CCAK-jv1**

ISACA