Keeping Secrets

In my last column,[1] I made the case that the protection of secret information—as opposed to personally identifiable information (PII)—is becoming a significant issue in cybersecurity. This article picks up where that one left off.

A secrecy program, added to that for privacy, necessitates a rather significant effort. Security professionals must build a protective program appropriate to the importance of their organizations' secrets. If those organizations happen to be military or intelligence agencies, there are surely such programs already in place. Of course, John le Carré would tell us that there is an equal and opposite program to steal that information, which is why a secrecy program is necessary in the first place. Moreover, civilian and commercial enterprises also have secrets and those need protection, too.

Fortunately, all these organizations have—or should have—information security functions that have been dealing for some time now with attempts to steal information. Much of the focus of these efforts has related to PII (i.e., privacy), so extending security to secrecy should not be much of a lift. But are the protections already in place for important information, including PII, sufficient for secret information? The answer to that question determines just how heavy the lift will be.

Secrecy Scenarios

For discussion's sake, let us consider three such secrets: the chief executive officer's (CEO's) holiday card list, quarterly financial results and the formula for a not-yet-patented wonder drug. What would happen if each of these were revealed? The CEO might be embarrassed if it were known who some of her or his friends are or who was excluded. Can the organization live with this embarrassment? Probably, but a head or two might roll.

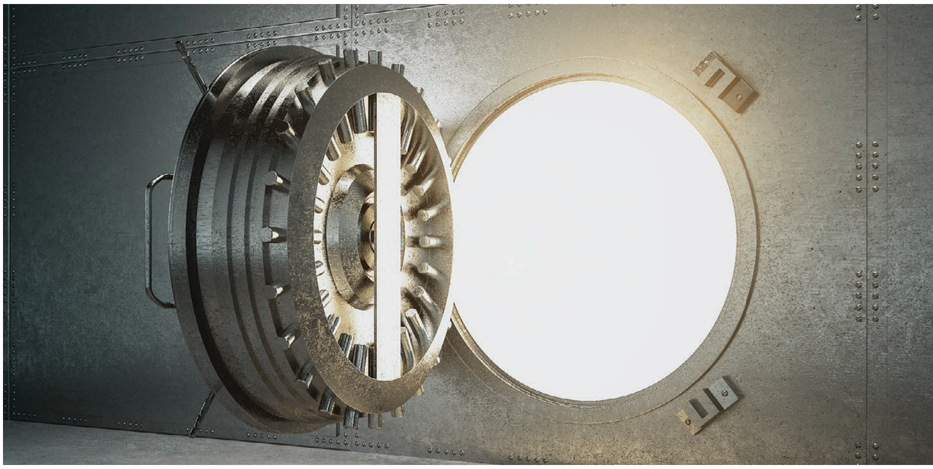
If financial results fell into the wrong hands just a few days too early, someone might make a killing in the stock market if the figures were particularly good or bad. This, in turn, could result in penalties from regulatory agencies, lawsuits and, perhaps, even prosecution if the perpetrator were someone with insider access.

In the case of the pharmaceutical compound, if the formula were stolen prior to patent protection, years of effort could be undone by a competitor that bypassed research in favor of theft. Add to that loss the cost of unrealized future profits, and the immense value of secrecy is apparent.

The point of considering these three scenarios is that information security professionals need to determine whether the "regular" security of information is sufficient for the particular type of secret information. In the first case, it probably is; in the second, maybe; in the third, probably not.

Security Strategies for Secrecy

This determination also is the basis for setting security strategies. One would take different approaches for short-term secrecy for information whose disclosure would cause embarrassment and long-term secrecy for information whose release might have life-or-death consequences. There is some information for which secrecy is felt to be so important that it becomes a part of the corporate culture. The recipe for Coca-Cola is probably the best known.[2] I doubt that sales of Coke would suffer if the formula were known, but the allure of



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.

secrecy is part of the brand and protecting it is worth a fortune to the company.

Of course, someone must have access to secret information and that person or persons must be known, identified and trusted. The factor of trust has always been the soft underbelly of information security. People are granted access to information because they are authorized to have it. If they abuse their authority, the security system has done what it was supposed to do but has, nonetheless, failed.

In principle, secrets should not be shared. But for practical purposes, they often must be. For example, the financial records of private companies are supposed to be confidential, but their bookkeepers and accountants know the information. When tax auditors come calling, the records must be divulged to them as well. So, part of keeping secrets secret is determining who may, can or must have access to them and who not.

Then security professionals must think like those in the "who not" category. In cybersecurity terms, the characteristics of attackers should be thought through, along with their motivations, inhibitors and attack vectors. The principle of *cui bono* (who benefits?) should be applied to project who the attackers might be; the understanding of the beneficiaries of disclosure—and their agents, such as criminals, terrorists and spies—should drive security strategy. And I submit that if the secrets are sufficiently important, a simple user ID and password are not enough.

Backing Up Secrets

Like all electronic information, secret or not, secrets must be stored in a secure place and must be backed up and stored securely somewhere else as well. Now, data thieves do not care if they get the prime or the backup copy. So an additional challenge in dealing with secret information is dealing with backups of secret information. Who will have the ability to access the secrets to back them up? How? Where will the backups be stored?

Dealing with secrets gets very messy, very quickly. For example, who will have the authority to retrieve them from backup storage? The same people who have access to the prime information or someone else? If it is the same people, might this undermine any provisions for dual custody protecting the information? If different people will have access to the backups, this expands the circle of trust around the secrets. Depending where the secrets are stored, there may well be persons with access who are not trusted employees, such as the personnel of a cloud service provider (CSP) or of a colocation facility.

> “OF COURSE, SOMEONE MUST HAVE ACCESS TO SECRET INFORMATION AND THAT PERSON OR PERSONS MUST BE KNOWN, IDENTIFIED AND TRUSTED.”

Legal Protections for Secrets

Have I been reading too many spy novels? They are not necessary; data theft is all over the newspapers. There are many examples including a few I will cite here:

- The woman who stole 100 million personal records from Capital One Bank in 2019 was a former employee of a CSP, and she was reported to have data from more than 30 other organizations.[3] Were any of them company secrets?
- A former engineer for a financial services company was convicted of trying to steal valuable proprietary computer code that took his employer years to develop.[4, 5] How many organizations have significant investments in their proprietary software?
- A freight car lessor operating in Russia was victimized by current and former employees who turned over financial information to the company's creditors, seeking some sort of vengeance.[6] Disgruntled employees with access to secret information are a particular threat.

These were three incidents that were thwarted and reported in the media. How many thefts of secret information have not even been discovered?

Legal prohibitions may have some deterrent effect on the theft of secrets. There are espionage laws that are applicable on the military side of the public sector and may be applicable on the civilian side as well. Trade secret laws can be used to prosecute data thieves in the private sector. But so what? I do not think that the people who are trying to steal secret information are unaware that it is illegal to do so. Anyway, many of them are beyond the reach of the jurisdictions in which the secrets are kept.

What should information security people do to protect secrets? I will continue this discussion in my next article and will address this question at that time.

Endnotes

[1] Ross, S.; "Secrecy and Privacy," *ISACA® Journal*, vol. 1, 2021, *https://www.isaca.org/archives*

[2] World of Coca-Cola, "Media Alert: Coca-Cola Moves Its Secret Formula," USA, 8 December 2011, *https://www.worldofcoca-cola.com/media-alert/coca-cola-moves-its-secret-formula/*

[3] Wakabayashi, D.; "Capital One Hacking Suspect Had Data From Other Targets, Officials Say," *The New York Times*, 14 August 2019, *https://www.nytimes.com/2019/08/14/technology/capital-one-hacking.html*. This was a breach of privacy, not secrecy. My point is that the incident related to a person with insider knowledge.

[4] US Attorney Office, Southern District of New York, "Software Engineer Arrested for Attempted Theft of Proprietary Trading Code From His Employer," US Department of Justice, 13 April 2017, *https://www.justice.gov/usao-sdny/pr/software-engineer-arrested-attempted-theft-proprietary-trading-code-his-employer*

[5] For the conviction, see United States District Court, Southern District of New York, United States v. Sazonov, Casetext, 16 February 2018, *https://casetext.com/case/united-states-v-sazonov*

[6] Justia US Law, OOO Brunswick Rail Management *et al*. v. Sultanov *et al*., No. 5:2017cv00017 - Document 15 (N.D. Cal. 2017), 6 January 2017, *https://law.justia.com/cases/federal/district-courts/california/candce/5:2017cv00017/306594/15/*