Steven J. Ross, CISA, 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.*

Cyber/Privacy

Twice in the past year or so I have received replacement credit cards because the numbers and expiration dates had been disclosed by merchants that I frequented. Each time, this resulted in about an hour of researching my credit card records, visiting the web sites of companies that I regularly pay via the card and updating my records. Surely, I am not the only one who has been affected. Multiply my lost hour by 70 million here, 40 million there, and sooner or later it adds up to some real inconvenience.

The merchants in question had not simply lost control of their customer records, nor did they publish my credit card information in the newspapers. They had been victimized by criminals who had penetrated their systems specifically to steal my data and that of millions of others; in other words, they had suffered a cybercrime. All the attention has focused on the crime; I am concerned here about the information.

INTRINSIC AND CONSEQUENTIAL IMPACTS

When information is stolen, it may have either *intrinsic* or *consequential* impact. In the former category, some lost information has value unto itself. Books and movies, for example, have intrinsic value. (When Sony was attacked last year, it was reported that in addition to crashing vital systems and publicizing embarrassing emails, the perpetrators stole several films. I am amused by the thought of the attackers—widely attributed to be North Koreans—sitting around and watching *Annie*.[1])

Indeed, stolen credit card numbers are said to have intrinsic value, since thieves sell them to yet other criminals, who then use the numbers and expiration dates to buy stuff.[2] In the case of stolen debit cards, the information is used to withdraw money from peoples' accounts. That is the consequential impact: what perpetrators can do with the information to create value for themselves once they have it. From my personal perspective, the net effect was inconvenience, but at a deeper level, it was a violation of my financial privacy. I have not seen much in the public discussion of cyberattacks to indicate an understanding that privacy violations have been the focal point of the most widely publicized attacks.[3]

GENERALLY ACCEPTED PRIVACY PRINCIPLES

The Generally Accepted Privacy Principles (GAPP)[4] is the definitive statement on data privacy. It defines privacy as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information." Considering the cybercrimes that have affected cardholders' financial privacy, perhaps GAPP can offer some insight into how privacy can be protected from cyberattackers. There are 10 principles.

Principle 1: Management

There must be an enterprisewide policy regarding privacy that must be communicated within the organization. Thus, privacy and, by extension, prevention of the breach of privacy are explicitly assigned to a designated person,[5] such as a chief privacy officer (CPO). I am not aware of any CPOs who are taking a leading role in cybersecurity and I would welcome communications to the contrary. That being the case, perhaps GAPP might be extended to require a chief cyber officer, part of whose mandate would be developing methods to protect data privacy against cyberthieves.

Principle 2: Notice

Organizations are supposed to notify data subjects about the purposes for which personal information is collected, used, retained and disclosed. No one is going to say, "We collect your credit card information in order to turn it over to criminals." But it would be nice to learn that my card had potentially been compromised at the time the merchant or the bank knew about it. My new credit cards just showed up in the mail.

Principle 3: Choice and Consent
Of course, I had no choice in the matter of whether my credit card information would be stolen, but I do have a choice as to whether or not to shop with merchants who do not protect me. Evidently, after the announcement of several major data thefts, customers have voted with their wallets to take their business elsewhere.[6]

Principle 4: Collection
My credit card information was used by criminals for purposes other than that for which it was collected by the merchants. But were the merchants' systems designed and used in a manner cognizant of the risk? Systems containing personal information should be subject to especially tight security.

Principle 5: Use, Retention and Disposal
My credit card is supposed to be used to buy things. If the information associated with the card was stolen one card at a time from a point-of-sale (POS) device, then this privacy principle was not violated. But if it was taken wholesale from unencrypted files, then the merchants' systems did not retain and dispose of the information in a proper fashion. Unfortunately, technical details on how some of the major retail cybercrimes occurred are sketchy at best. From press reports, it would seem that both POS terminals and central servers have been the source of the stolen information.

> "The underlying vulnerability of information systems is not inferior security, but inadequate software."

Principles 6 and 7: Access and Disclosure to Third Parties
My ability to access, review and update information about myself has nothing to do with cybercrime. Neither does the disclosure provision. While giving my personal information to crooks fits under this principle, I doubt that it was what was meant by the authors.

Principle 8: Security for Privacy
This principle, as applied to cybercrime, is exactly what the authors had in mind. Prevention of unauthorized access, either physical or logical, is what current IT practices evidently fail to do. In light of all the cyberattacks that have happened, it seems that access control systems are being used to keep the honest honest. Keeping out well-funded, dedicated cyberthieves has proven as effective as the Maginot Line (more on this in a future article).

Principle 9: Quality
The authors of GAPP defined quality as the maintenance of "accurate, complete and relevant personal information." That is not what I mean by the term and it is not how I would apply this principle to privacy protection in the age of cyberattacks. As I have written previously, I believe that the underlying vulnerability of information systems is not inferior security, but inadequate software.[7]

Principle 10: Monitoring and Enforcement
One of the most maddening aspects of major thefts of personal information, according to media reports, is that in many cases the losses occurred for lengthy periods of time before the organization under attack even realized it. For just one example, the US Office of Personnel Management (OPM) notified its personnel in July 2014 that a breach of personnel records had occurred in March of that year.[8] Then, in June of 2015, OPM announced that 4 million records were taken, which by July had been raised to 21.5 million.[9] I do not know precisely how the breach occurred, but I do believe that someone should have noticed it was going on the moment it happened. The technology is there for that purpose and evidently it was not used, because the computer systems were too old.[10]

CONCLUSION

There is a lot to be learned by considering certain cyberattacks as privacy violations. GAPP offers some guidance, but the principles are not a tight fit with the cybertheft of personal information. Will organizations apply those lessons? That remains to be seen.

ENDNOTES

[1] Sakoui, Anousha; "Sony Films 'Fury' and 'Annie' Said Stolen in Cyberattack," *Bloomberg Business*, 29 November 2014, *www.bloomberg.com/news/articles/2014-11-30/sony-films-fury-and-annie-said-stolen-in-cyberattack*

[2] Hackett, Robert; "Online, a Bazaar Bursting With Stolen Credit Card Information," *Fortune*, 21 September 2014, *http://fortune.com/2014/09/21/home-depot-stolen-card-information-market/*

[3] Interestingly, the *Preliminary Cybersecurity Framework* issued by the US National Institute of Standards and Technology contained a section on a "Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program" that was eliminated in the final version issued in February 2014.

[4] American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy Principles, August 2009. ISACA® and the Institute of Internal Auditors were also contributors to this document.

[5] *Ibid*., p. 13. The document referenced here is the version for business people, not the one for accounting practitioners.

[6] For example, see Target, "Target Provides Update on Data Breach and Financial Performance," press release, *http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.*

[7] Ross, Steven J.; "Microwave Software," *ISACA® Journal*, USA, vol. 1, 2015

[8] Email reproduced in the *Washington Post*, "E-mail to OPM Staff on Security Breach," 10 July 2014.

[9] Bisson, David; "The OPM Breach: Timeline of a Hack," *Tripwire*, 29 June 2015, *www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/*

[10] C-SPAN, Testimony by the Office of Personnel Director Katherine Archuleta, *www.c-span.org/video/?326767-1/opm-director-katherine-archuleta-testimony-data-security-breach*