Fifty Years of Information Security

A Recollection

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2PpWxZ6

This being the first issue of the *ISACA® Journal* of 2019, which happens to be ISACA's 50th anniversary, the kindly editors asked me to write a history of information security over the past half-century and, oh by the way, in less than 1,500 words. I politely, but firmly, declined. I have not been in the field for quite all those years. My experience has been in the commercial sector, and I know next to nothing about information security in the military, nor in academia for that matter. So the best I can offer is my recollections about how things have changed in information security over the course of my career.

The Data/Information Security Function

I began as the data (not information) security officer in a Wall Street bank after a stint in electronic data processing (EDP) auditing (such as it was called then). I had audited information security and found it wanting, so I was appointed to fix it. At the time, one other bank had a security official and, shortly thereafter, he quit, so, for a few months, I was the only one in US banking. It is hard today to conceive of banks, which are, after all, where the money is,[1] not having at least one person focused on the security of their computer systems and data. Almost without exception, major (and many not so major) organizations have someone with a title of chief information security officer (CISO) or something like it. I cannot say with authority when the ubiquity of CISOs began,[2] but I am pretty sure it was the case in this century. I had quite a run of consulting projects setting up information security functions; the last was in 2005.

The CISO title is instructive. It denotes a level of seniority and respect that was not the case back when. The main information security task in the earliest days was the issuance of what we would call credentials, but was then called "password administration." Yes, I gave out user IDs and passwords(!), which I stored in the clear in case the recipients forgot them. It was the best security we could get with the technology in use. Having a role in policy and procurement was a fantasy at first, although I must say that I and my colleagues in the field gained such a role rather rapidly. This may have had a lot to do with some well-reported frauds[3] that occurred at the time.

Fraud, Hacking and Cyberattacks

It is timely to remember that once the perception of what the bad guys were doing was fraud, not hacking or attacks. This progression is more than linguistic. It is understood when using the word "fraud" in this context that the fraudster is misusing the system in such a way as to acquire something of value external to the system (such as money or diamonds). "Hacking" as a term for external misuse of a system first achieved currency in the 1980s, although it had been used that way earlier.[4] Importantly, a hacker was not thought to be seeking to get something, but rather to sow disruption and confusion as widely as possible. These days, a "cyberattacker" is seeking to obtain something from within the system, not outside it. That something, of course, is data or the targeted downfall of the system (and its owner).

Steven J. Ross, CISA, 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.

In the early years of commercial information security, the idea that organized groups from governments or criminal gangs would attack information systems was the stuff of thriller fiction and comic books.[5] To be fair, the great Donn Parker warned us about all this in his book, *Crime by Computer*, in 1976.[6] And yet, forewarned, we allowed it to happen. The entire history of information security seems to be one of continual shortcoming. We have always been trying to catch up to the latest threat.

Information Security Tools

Over the years, there has been a plethora of tools that have promised to close the gap. In the era of centralized mainframe systems, the most important of these were access control systems. For the most part, they ran on IBM 370-era mainframes with top-end operating systems, because these dominated the computing market. If your organization was using computers from NCR, Univac[7] or other manufacturers long out of the mainframe business, products for use were hard to come by. Today, access control is built into operating systems and administered by technicians, not information security professionals.

> "ENCRYPTION WAS, AND STILL IS, THE SOLE INFORMATION SECURITY TOOL THAT PROTECTS THE DATA RATHER THAN ACCESS TO IT."

Encryption was, and still is, the sole information security tool that protects the data rather than access to it. The Data Encryption Standard (DES) was sufficient for quite a while, from 1976[8] to 1999.[9] It was replaced by the Advanced Encryption System (AES), which was, like DES, a symmetric key system. Then came asymmetric public-key encryption systems, which, along with AES, are still in use.

The problem is that encryption is not used widely enough. Or rather, it is not used as an explicit security tool. It is embedded in many products and network services. Still, it has never reached the widespread application expected of it, largely because improved algorithms have not been matched by improved systems for managing encryption keys.

Recognition of the Importance of Information Security

The most positive trend I have observed during my decades in the profession is the general recognition of the importance of information security. In the beginning, it was just ignored. The tales of passwords posted on terminals and shared by departments were never apocryphal. I saw them with my own eyes. Those days are long past. I think. I hope.

It was hard to explain to acquaintances (or my own children) what I did for a living. The general impression was that I was trying to build a very large solution to a very small problem. Then, in 1983, Fred Cohen coined the term "computer virus" and the public's perception of the threat became crystallized. Maybe all we needed was better marketing. This was followed by the Morris worm,[10] Kevin Mitnick's trail of hacking attacks,[11] the Melissa virus[12] and the incursions during the 2016 American presidential election. (Feel free to add your favorite security horror story to this list.) All that plus cyberattacks and both the general public and organizational management now get it. Better marketing, indeed. Ironically, it took repeated incidents of information insecurity to gain our profession the recognition it deserves.

Endnotes

1 Answer to the question, "Why do you rob banks, Willie?" asked of Willie ("the Actor") Sutton. Going straight to the obvious is now known as "Sutton's Law."
2 But I can say who the first CISO was. He was my friend Steve Katz, then of Citibank.
3 For example, Equity Funding (1973); Stanley Rifkin robbing Security Pacific Bank. You want to know more? That is what Google is for.
4 Yagoda, B.; "A Short History of 'Hack,'" *The New Yorker*, 6 March 2014, *https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack*

Enjoying this article?

- Read *Cybersecurity Fundamentals Study Guide, 2nd Edition. www.isaca.org/cybersecurity-fundamentals-study-guide*
- Learn more about, discuss and collaborate on information security management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

5 Where is Lex Luthor, that criminal mastermind? Perhaps he is behind all these cyberattacks?
6 Parker, D.; *Crime by Computer*, Scribner, USA, 1976. This book is still available.
7 I realize that the foregoing is rather US-centric. These are my recollections, after all.
8 When the US National Bureau of Standards (nowadays called the US National Institute of Standards and Technology [NIST]) accredited it. See US Department of Commerce/National Institute of Standards and Technology, *Federal Information Processing Standards (FIPS) FIPS Pub 46-3, Data Encryption Standard*, USA, 1999, *https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf*
9 When DES was first cracked in a reasonable time period. See Van Zande, P.; "The Day DES Died," SANS Institute, 2001. NIST withdrew DES in 2005.
10 Lee, T. B.; "How a Grad Student Trying to Build the First Botnet Brought the Internet to Its Knees," *The Washington Post*, 1 November 2013, *https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?noredirect=on&utm_term=.5af91f3c066e*
11 Sinha, C.; "Infamous Hacker Kevin Mitnick Tells Us How He Created Fake Identities," *Motherboard,* 18 June 2017, *https://motherboard.vice.com/en_us/article/d38mjz/infamous-hacker-kevin-mitnick-tells-us-how-he-created-fake-identities*
12 Ross, S. J.; E. L. Quah; "Who Is Melissa Chernobyl and Why Is She Doing These Terrible Things?" *IS Audit and Control Journal*, vol. 4, 1999. One of my first articles in this space.