Why We Failed

Near the end of a recent column I mentioned, almost off-handedly:

> *The last time there was a shift…in the way information technology was organized occurred when we moved from massive centralization—mainframes to distributed processing. Candidly, we security professionals did not manage that one well.*[1]

That statement crystalized in my mind some thoughts that had been nagging at me for a while. Girish Desmukh wrote to me from Pune, India, and called me out on what I had written: “Can it be possible for you to give a few examples about what happened when security was undermined during the move towards decentralized processing?” Well asked, Mr. Desmukh, and worthy of a public response.

Security in the Distributed Era

At the time I wrote the sentences I quote, my thoughts on the subject were not clearly articulated in my head, nor was the logical follow-on to what I wrote. In considering these afterward, I realize that there are many signs that information security is not where it should be. In particular, the ubiquity of cyberattacks underscores that those of us who have the professional responsibility for the security of information systems have failed in our mandate. Yes, that is a very stark statement, but to me, the evidence is overwhelming. From the time that distributed systems overtook centralized computers as the dominant architecture for managing information, there has been a constant stream of viruses, worms, denial-of-service attacks, botnets and cyberattacks that have plagued organizations large and small, public and private. We have, to an extent, been able to mitigate these threats, but not enough to claim meaningful success.

Taking a broad historical view of information systems, there have been two eras: centralized (roughly, 1950-1985) and distributed (1985-present). In the first, centralized era of computing, we were certainly concerned about security, and there were breaches, but not nearly of the frequency and magnitude we face today.[2] As distributed systems took hold, so did the problem of massive security failures.[3] They have continued to grow in sophistication and impact to this day.

Professional Influence

We might have been able to halt the profusion of security problems if information security professionals had more influence in their organizations in the early days of distributed systems. In many cases, even in large organizations, the head of the information security function was the first person in that position and was often a staff of one. It has taken a generation for the chief information security officer (CISO) to gain organizational prominence, largely driven by the increased understanding by top management that threats to information systems are strategic in nature. It is ironic that this increased prominence has come about because we in information security have been unable to stanch the flow of system insecurity.

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/2O1W5A1

Steven J. Ross, CISA, CISSP, MBCP 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?

- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/Information-Security-Management*

Centralized Security for Distributed Systems

Almost all of the early leaders in the information security field learned their craft on mainframe systems. And so, they attempted to impose a centralized security model on a distributed architecture where it never quite fit. That is because there was no central point at which access controls and other security measures could be applied. Precisely because they are distributed, systems can communicate with other systems and pass control among themselves. I have many times asked security professionals for a description of the interactions of the systems for which they were responsible. I have received spaghetti diagrams, if they had any at all. Such a mishmash cannot be secured centrally.

Searching for the Magic Button

To a great extent, we in information security have spent the last 30 years searching for a magic button—that one software package or technique that would solve the security problem. We were conditioned for such a search because we had one in the centralized era. Access control facilities for mainframe computers were introduced in the mid-1970s, and they really did provide an effective tool for implementing security—a centralized solution to a centralized problem.

> “IN LARGE MEASURE, INFORMATION SECURITY WILL NEVER BE ‘SOLVED,’ BECAUSE SOLUTIONS ARE FINITE AND THE PROBLEM IS UNBOUNDED.”

There is no equivalent in the distributed era, although Active Directory (AD) comes close. However, AD works only in Microsoft Windows environments, and many distributed systems run on platforms other than Windows. Moreover, the well-publicized security flaws in successive versions of Windows[4] undermine the effectiveness of AD.

There has been no dearth of panaceas, including antivirus software, firewalls, public key infrastructure (PKI),[5] encryption, intrusion detection and prevention, and, latterly, blockchain[6] technology. Each has had its purposes; some have been widely utilized; others have been overtaken by time. None has “solved” information security.

In large measure, information security will never be “solved,” because solutions are finite and the problem is unbounded. Neither systems nor user populations are static. If today every individual were able to access only the systems and information for which he or she was authorized, tomorrow there would still be new systems, new users and new sorts of malicious attacks. The conundrums of authorization, identification and protection will always remain. The magic button will not be found because it cannot exist.

Risk Management and Economics

The degree to which solutions can be approached is limited today more by risk management and economics than by technology. Security professionals have been raising an outcry about the risk of cyberattacks for years. However, the economic consequences, while grave, have not been borne out at a macro level.

As security breaches have become increasingly commonplace, the consequences have been shown to be less severe than we security folks have predicted. One scholar has noted that it is rare for an attacked organization to be financially constrained.[7] It is not only that almost all of the victims of cyberattacks have stayed quite comfortably in business; their stock prices went down briefly and then returned to where they were before the attacks or have even risen. Corporations have less incentive to invest in prevention if they know their stock price will survive. This reluctance takes a toll on the overall economy and consumer privacy.[8] But information security leaders have been hard-pressed to demonstrate more than marginal improvement for additional money spent.

So, the best that can be said is that the most secure organizations today are as secure as they can be, given the constraints of finances and technology. The management of each organization must decide whether that is secure enough. The community of information security professionals must determine whether we can improve on what we have accomplished in the past 35 years or so. It is my opinion that we have backed ourselves into a corner: We cannot substantially improve security without making fundamental changes to the underlying architecture we are trying to protect.

> “WE CANNOT SUBSTANTIALLY IMPROVE SECURITY WITHOUT MAKING FUNDAMENTAL CHANGES TO THE UNDERLYING ARCHITECTURE WE ARE TRYING TO PROTECT.”

Author’s Note

I am no fan of articles that point out a problem but offer no ideas as to what to do about it. This article is one of those. My only excuse is that I have run out of the room that the editor has allotted me. I promise that, having spoken to why we failed, I will address how we might succeed in the next issue.

Endnotes

[1] Ross, S.; “Security in the Migration to a Multi-Modal Environment,” *ISACA® Journal*, vol. 3, 2018, *www.isaca.org/archives*

[2] The manufacturer of the operating system most widely used then by large enterprises was able to claim that it would prevent any bypasses of security. Of course, the manufacturer did not accept responsibility for consequential damages, only that it would fix any flaws. Nonetheless, such a warranty is more than other vendors are willing to offer today. See Viz. IBM z/OS® System Integrity Statement, *ftp://public.dhe.ibm.com/s390/zos/racf/pdf/zOS_System_Integrity_Statement.pdf*. I was unable to find the original 1973 statement on the web.

[3] I would say that the first of these occurred in 1988, the early years of the distributed era. It was the so-called Morris Worm, which brought down thousands of computers on the Internet at the time when the Internet was little more than a small town where people thought little of leaving their doors unlocked. 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*

[4] Publications on this topic are too numerous to list here. See CVE Details for 50 reported flaws in Windows 10 alone, *https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html*.

[5] My first article in this space was Ross, S.; “If PKI Is the Answer, What Is the Question,” *ISACA Journal*, vol. 4, 1998. I have been a skeptic for a long time.

[6] Blockchain shows great promise for some applications, but is not a universal security solution. I have great confidence that, in time, someone will find a way, if not to break blockchain, to go around it.

[7] Stultz, R. M.; “What Is the Impact of Successful Cyberattacks on Target Firms?” Harvard Law School Forum on Corporate Governance and Financial Regulation, 30 March 2018 *https://corpgov.law.harvard.edu/2018/03/30/what-is-the-impact-of-successful-cyberattacks-on-target-firms/*

[8] Kvochko, E.; R. Pant; “Why Data Breaches Don’t Hurt Stock Prices,” *Harvard Business Review*, 31 March 2015, *https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices*