How We Can Succeed

In my last article, I excoriated the information security community, of which I am a card-carrying member, about the state of security today. Moreover, I stated my opinion that the underlying architecture of distributed systems, the most commonly implemented since the late 1980s, is incapable of supporting a tolerable level of security. Thus, we have suffered through viruses, worms, denial-of-service (DoS) attacks, botnets and cyberattacks for more than a generation.[1]

> "RECOGNITION OF THE TOTAL COST OF OWNERSHIP DRIVES ORGANIZATIONS TOWARD THE CLOUD. THE QUESTION OF BUILD VS. BUY IS PASSÉ; TODAY, IT MAKES SENSE TO RENT."

A New Era

Just as the distributed model displaced the centralized (i.e., mainframe) one, I now believe that we are on the threshold of a new era, that of a multi-modal, utility, cloud-based, commercial, Software as a Service (SaaS) (choose any two terms at your pleasure) architecture. Both ownership and geography differentiate the "utility SaaS" architecture from those that went before.[2] In the centralized era, ownership of data and software rested within the organization, which kept both of them in one big room. In the distributed era, i.e., today, the organization still owns the data and software, but these may or may not all be in the same place. In the cloud-based multi-modal environment that is now arriving, the organization retains ownership of the data, but not the software, nor does it house the computing.

Many core business functions are routinely being performed or supported in the cloud and have been for several years. For example, organizations increasingly turn to commercial services for customer relationship management (CRM), payroll, human resources (HR), order entry, accounting, inventory, supply chain and many other automated business functions. The economics of using cloud-based services just make sense. No single organization can afford to have staffs of specialists to develop and maintain software for each function in the way that a vendor specializing in that function can do. Recognition of the total cost of ownership (TCO) drives organizations toward the cloud. The question of build vs. buy is passé; today, it makes sense to rent.

Security in the Commercial SaaS Environment

The same point, overwhelmingly, applies to information security. No organization that I am aware of has a team of security professionals for each application. But, for cloud-based service

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/2pBRr1q

Steven J. Ross, CISA, CISSP, AFBCI, 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 ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

vendors, this is a commercial necessity. The incentives for a vendor's security include not just financial, legal, reputational and regulatory risk—as though those were not enough—but existential risk as well.[3] The inability of a cloud-based software vendor to implement and maintain security over its products and services will likely put it out of business.

Zero Trust

In fairness, using a variety of cloud-based services does not an architecture make. And well-secured applications do not by themselves make the entire environment safe. More is required before we can say that we have improved significantly on the shortcomings of the distributed era.

> "AS INCREASING NUMBERS OF APPLICATIONS ARE BEING USED AS CLOUD-BASED SERVICES, ORGANIZATIONS ARE REALIZING THAT THEY ARE DEALING WITH TOO MANY CLOUDS."

In several previous articles in this space, I have referred to the Zero Trust Model.[4] It is not exactly a standard, although it has the imprimatur of the US National Institute of Standards and Technology (NIST), in a publication called "Developing a Framework to Improve Critical Infrastructure Cybersecurity."[5] In a very brief synopsis, in the Zero Trust Model, all networks—and, by extension, the information systems on the network—are *untrusted*. All resources are accessed securely regardless of location. Access to resources is based on a least-privilege strategy and access controls are strictly enforced. All network traffic is inspected and logged.[6]

The architecture that can be built on the Zero Trust Model is based on a segmented network with all security-related controls established at a single point of entry and transfer. These controls constitute a unified threat management gateway. In practice, this gateway is a "next-generation firewall" (NGFW), sold by many equipment manufacturers.[7] By itself, NGFWs are necessary but insufficient for effective security. A secure architecture must be based on rigorous network segmentation such that a user authorized for one domain cannot traverse the network without returning to the access control mechanism. That mechanism must include what some have called "next-generation access" (NGA), with advanced functionality such as correlation of users and uses, machine learning to identify anomalies, and technical integration with the security features at the network level.[8] The complete implementation of the Zero Trust Model is being referred to as the Zero Trust Extended Ecosystem (ZTX).[9]

Getting to Success

This is all wonderful in theory, but organizations are not about to re-architect their entire IT environment around an enhanced security. But they are migrating to multi-modal environments as a pathway that can lead to ZTX, *if information security professionals exert their influence now*. As increasing numbers of applications are being used as cloud-based services, organizations are realizing that they are dealing with too many clouds. They are seeking a "cloud of clouds," one cloud to control them all.[10] And that is where the Zero Trust Model can be implemented.

Let me paint a word picture of what I believe is the future of information security. All uses of information are defined in domains, and all users are associated with one or more domains. All security controls are embedded in a central control point (the cloud of clouds). An authenticated user can proceed to a domain and do what he or she is authorized to do *and nothing more*. To do anything else, the user must return to the control point and be reauthenticated and reauthorized. All of these accesses are recorded and analyzed at the control point and any anomalies are reported.

The roles of information security professionals will be transformed from passive policy making and active implementation to that of vendor management and security monitoring. One very positive sign that this transformation has begun is that many information security professionals are already involved in, and occasionally arbiters of, SaaS acquisition decisions.

I am not so naïve as to think that all this wonderfulness will arrive due to a sudden enlightenment in the executive ranks. To be sure, some of it will occur because of the persuasiveness of chief information security officers (CISOs). I think a lot more will happen because organizations will back into intolerable situations with uncontrolled acquisition and use of services, with only ZTX as a way out. And some will happen because, at long last, the zeitgeist is ready and willing to pay for secure computing. I am convinced that this is the way in which we information security professionals will succeed.

And then, when that happens, I will not be able to author this column because there will be nothing to write about. Nah. There will always be new challenges. Keep your seat belts fastened; it could be a bumpy flight.

Endnotes

1 Ross, S.; "Why We Failed," *ISACA® Journal*, vol. 5, 2018, *https://www.isaca.org/archives*

2 I realize that the dates of these eras are approximations. Mainframes did not disappear in 1985; in fact, they are not gone today. And the cloud did not suddenly spring into existence in 2015. The fact that boundaries are fuzzy does not mean that they do not exist. A highly unscientific search for the first mention of "the cloud" came up with "The Self-Governing Internet: Coordination by Design," by S. Gillett and Mitchell Kapor (yes, the Mitch Kapor of Lotus) in January 1996 (*http://ccs.mit.edu/papers/CCSWP197/CCSWP197.html*).

3 Cytryn, A.; E. Beck; S. Ross; "Hackers, Snoopers, and Thieves: How to Handle the Latest Threats," *Journal of Corporate Accounting & Finance*, June 2014, *https://onlinelibrary.wiley.com/doi/abs/10.1002/jcaf.21972*

4 Ross, S.; "Bear Acceptance," *ISACA Journal*, vol. 4, 2014, *https://www.isaca.org/archives/*

5 Forrester Research, "Developing a Framework to Improve Critical Infrastructure Cybersecurity," USA, 2013, *https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf*

6 *Ibid*., p. 5

7 One such manufacturer has published a guide to implementing the Zero Trust Model with its products. Palo Alto Networks, "Designing A Zero Trust Network With Next-Generation Firewalls," *https://media.paloaltonetworks.com/documents/zero-trust-solution-brief.pdf*

8 Cunningham, C.; "Beyond Zero Trust: Next-Generation Access," *ZDNet*, 11 April 2018, *https://www.zdnet.com/article/next-generation-access-and-zero-trust/*

9 This term is espoused by Forrester Research. Cunningham, C.; S. Balarousas; B. Barringham; P. Dostie; "The Zero Trust eXtended (ZTX) Ecosystem," Forrester, 19 January 2018, *https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210*

10 There are many references to a cloud of clouds in the literature. For an easy-to-read overview, see Alvarez, L.; "The Second Digital Revolution: A Cloud of Clouds," ITProPortal, 15 January 2016, *https://www.itproportal.com/2016/01/15/the-second-digital-revolution-a-cloud-of-clouds/*.