Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

Microwave Software

Let me tell you about my microwave. When I bought it, it was called a microwave oven and I was going to roast turkeys in it in half an hour. I am sure it was white then, but it has turned a pale, sickly yellow. I never did cook a turkey in it and all I ever use it for now is to defrost sauces, reheat coffee and nuke the ice cream so it is soft enough to scoop. Even though it is more than 20 years old, it still works and it does what I need it to do, so there is no reason to buy another with a lot of features in which I have no interest.

I am certain that the data centers in every organization older than 20 years have applications running in them that are just like my microwave. They are old software serving a limited purpose, often for a limited number of business functions (or for just one). They work; they do what their users want them to do, thus there is no reason to buy a new system with a lot of features in which those users have no interest. Ominously, they are indicative of the reason that the problems of cybersecurity will not be solved any time soon.

SOFTWARE, OLD AND NEW

As I was writing this article, a news report announced the discovery of a flaw in a widely used software product called Bash. It is freeware that is incorporated into 70 percent of the machines that connect to the Internet. Created in 1987, the software has been maintained by a volunteer, who evidently introduced the flaw in 1992. According to the report, the bug, known as Shellshock, can be used to take over entire devices, "potentially including Macintosh computers and smartphones that use the Android operating system."[1] Ubiquitous software with a flaw undetected for 22 years! If ever there was microwave software, this is it.

Corporations and government agencies have accumulated their application portfolios over a period of years. Many still have programs written in COBOL, running on mainframe computers and written when most of their employees were in grade school. Others modernized their systems in anticipation of the new millennium, now 15 years behind us. In many companies, applications exist because they served a predecessor corporation that has long since been acquired and absorbed, but which lives on in ancient software. Each of these applications operates atop an infrastructure, often shared with other programs. They each get data from somewhere and send results somewhere else. If not well controlled, they expose those data to theft and misuse.

It is my experience that very few organizations know how all their applications work, which programs they interface with, or how they use operating system and middleware services. Yes, that is an over-broad generalization, and, yes, there might be some organizations that understand all their systems—all of them, no exceptions, 100 percent. But I stick to my assertion—just because it is a generalization does not make it wrong.

Here is the challenge: Are all applications, data and infrastructural elements[2] protected at the same level? Or do the "critical" systems receive the greatest security, control, recoverability and audit attention, while the rest are relegated to "tier 2"? As I said in different context in a previous article, there is no such thing as tier 2.[3] Small, lightly used, nearly forgotten systems may be running on the same platforms or in the same highly interconnected infrastructures as those depended upon by large numbers of users for essential business functions. If they are not protected as though they were critical, these systems can expose the ones that are more highly valued when a cyberattacker comes along looking for a weak spot to penetrate.

IT IS ONLY

Beware the "Oh, it is only…" response. It is only the forecasting system, which, if illicitly tweaked just a bit, causes a manufacturer to over- or undersupply products to the marketplace. It is only the training system that enables sensitive tasks to be staffed just by qualified personnel. It is only the library system that can be used to display—or to hide—

information critical to lawmakers. These are not randomly chosen examples, nor are they hypothetical. They are the equivalents of my microwave, sitting on the kitchen counter or in the data center or the office or the store for so long that they are hardly noticed. But cyberattackers notice and exploit them. For example, the instrument that caused so much damage to Target and Home Depot was not a server array. It was *only* a cash register.[4]

The problem of cyberthreats is not going to be solved[5] just by replacing microwave software with gleaming new products. Newness is not enough. Should some technoarchaeologist read this piece 20 years hence, I am sure he/she will chuckle about some buggy software introduced in 2015. The fact is that in any significant enterprise, there are so many programs acquired over such a wide span of time, developed to run on so many different infrastructures, that there are almost certainly going to be holes in the code and in the interfaces of which a patient attacker might take advantage. Advanced persistent threats (APTs) reward just such patience.

THE HEART OF THE MATTER

The jumble of systems, new and antiquated, well and poorly controlled, leads me to conclude that: Cyberthreats are not a security problem. They are a systems problem.

> Cyberthreats are not a security problem. They are a systems problem.

There is only so much information security professionals can do to build barriers and walls and fences and domes around information systems and data. Ultimately, flawed software cannot be secured. It can only be made more difficult—not impossible—to penetrate.

Those responsible for information systems, beyond the chief information officer (CIO) up to the highest ranks of management, must accept that cyberattacks will occur and that some of them will succeed.[6] That being the case, an equal investment should be made in preparing for recovery from such attacks as is given to preventing and detecting them. The *Framework for Improving Critical Infrastructure Cybersecurity*[7] lists "recover" as one of the five functions of cybersecurity. However, I have seen very little money spent on recovering from cyberattacks. This will have to change.

The most important step, to my mind, in mitigating the threat of cyberthreats is for organizations to gain a thorough understanding of all the software running in their environments, the flow of data and control among them, the interfaces among them and within their infrastructures, and the exposures presented by what I have termed microwave software. In too many organizations, neither management nor staff knows these things. Their ignorance is bliss for the malefactors in the darkest regions of our hyperconnected world. They are looking for and finding such exposures. This should be all the incentive required for legitimate organizations to become, at least, aware of what is running in their data centers and, at best, to make all the software—both up to date and microwave—work harmoniously and safely together.

ENDNOTES

[1] Perlroth, Nicole; "Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant," *The New York Times*, 24 September 2014, *www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html?module=Search&mabReward=relbias%3Ar%2C%7B%221%22%3A%22RI%3A9%22%7D*

[2] Better known as "configuration items" in ITIL terminology. See ITIL, *www.itil-officialsite.com/InternationalActivities/TranslatedGlossaries.aspx.*

[3] Ross, Steven J.; "Shedding Tiers," *ISACA Journal*, vol. 2, 2014

[4] Kuchler, Hannah; "Home Depot Attack Bigger Than Target's," *The Financial Times*, 19 September 2014, *www.ft.com/cms/s/0/7f9a2b26-3f74-11e4-984b-00144feabdc0.html#axzz3EMhI2Uy9*

[5] I am not even sure that there will ever be a solution as such. As technology advances, so do the tools and incentives for those who would undermine information systems. If we cannot win the war, we can at least reduce the number and severity of casualties.

[6] See my previous article: Ross, Steven J.; "Bear Acceptance," *ISACA Journal*, vol. 4, 2014.

[7] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 12 February 2014