The End of the Beginning?

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.

At each stage in the evolution of information security, there has been a problem—access control, viruses, hackers, data leakage, to name a few—that has seemed insuperable. Then, little by little, the community of information security professionals came to grips with the problem. They did not eliminate it, but they contained it and made it manageable. After all, we are still confronted by unauthorized access, nasty malware, script kiddies and misused data, but we are able to continue to use information systems and The-End-of-Civilization-As-We-Know-It has not occurred, despite frantic contemporaneous predictions of chaos.

The most recent subject matter of the Doom and Gloom Brigade is cyberattacks.[1] Now, these really are different because they are deliberate, targeted, malicious attempts to harm specific organizations, perpetrated by governments, criminals and terrorists with large reserves of time, money and expertise. But I am convinced that, as large as the problem might currently be, the information security community will eventually contain and manage the problem of cyberattacks. Eventually, yes, but when?

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.

Well, maybe eventually is now. With a bit of head-above-the-bunker bravery, or foolishness, I would like to suggest that we may be seeing, to paraphrase Winston Churchill, not the beginning of the end, but the end of the beginning.[2]

What brings on this burst of sunny optimism? IBM has reported statistics on cyberattacks showing a decline from 12,017 in 2014 to 1,157 in 2015.[3] The Ponemon Institute's annual assessment of the cost of data breaches indicates that in Germany and the United States, the rate of increase in cost has slowed over the period from 2013 to 2015 and has actually declined in Australia and the United Kingdom.[4] Symantec also publishes an annual study of Internet security threats, which reports a 2 percent increase in the number of data breaches in 2015, compared with a 23 percent increase the year before.[5]

Now, one swallow does not a summer make, but three reports of declining rates or actual decreases may be early indicators of a trend. Let us, for the sake of this article, assume that it is so. Since we can reasonably suppose that the cyberbaddies have not had a sudden spurt of virtue, maybe those of us trying to prevent cyberattacks are having a positive effect. What are some of those things that are creating this favorable trend, if a trend it is??

Acceptance

Several years ago, I wrote in this space that acceptance by senior management and boards of directors of the threat of cyberattacks was the key to generating the budgets to counter the threat.[6] There is little doubt in my mind that this has been accomplished. Numerous news reports, research studies and publications[7] have made the reality of cyber security incidents clear to those holding the purse strings.

Understanding does not necessarily lead to action, but I believe, in this instance, it has. As a veteran information security professional, I believe the case for cyber security preparations makes itself. The media reports by themselves did not convince decision makers that countermeasures were required. If anything, they raised questions about why existing safeguards were insufficient. But acceptance of the reality of cyberthreats gave information security management a receptive audience when the case was made.

Technology

Where money is to be made, the market will respond, and it has. There are hundreds of products and services available[8] that purport to be the solution to cyberattacks. Many of these, so I have found, are merely repackaging of existing tools and technologies, but that is relatively unimportant. The technologies were not previously being bought, implemented and used (or at least not for cyber security purposes). If it takes a bright new label and an avid salesman to get the right tools into the hands of the right people, that is just fine with me.

As I parse the marketplace, I see roughly a third of the top products providing prevention, about a quarter detection and analytics, and the rest splintered among risk management, services and testing. Shockingly, to me at least, there are no products in the marketplace for recovery from cyberattacks. I think there is a great product opportunity there if—a significant if—there are buyers waiting for the market to respond.

In so many organizations, information security and disaster recovery are in different management chains, and the budgeted funds are not flowing in the direction of recovery. Perhaps it is just that the promise of prevention overwhelms the reality that even very well-protected companies and government agencies have experienced cyberattacks. No matter how strong the preventive and detective tools may be, the attackers have the luxury of time, money and patience. Attacks will happen to the well prepared and the unprotected, so cyberrecoverability needs to be a part of every organization's armory.

The Cloud

More and more organizations are migrating more and more applications and infrastructure to the cloud. This may be little more than outsourcing or it may be a complete revision of their IT architectures, but it seems that there has been a positive, perhaps unintended, side effect: Security has been improved. Providers of outsourced IT services have a strategic interest in information security generally and in cyber security specifically. Most of us information security professionals provide support for systems that, in turn, support business processes. We do not make loans or steel or candy for a living; we help make the information the business people use more reliable and available. Even if information security is breached, the products retain their value. Cloud providers are in the business of information systems; the systems are their products. Therefore, breaches of security—particularly those in which customer data wind up in nefarious hands—undermine the market potential of the cloud companies themselves. As was stated by a colleague of mine,

> *Cloud and Software as a Service (SaaS) vendors…clearly have the resources and capabilities to provide safe environments. Their technical resources are unprecedented in many ways, as demonstrated by the way in which Cloud and SaaS vendors have developed innovative systems using generic, low-cost servers which now threaten the businesses of major well-capitalized leaders in technology. Presumably, they have the ability as well to secure their services and data. They have a commercial incentive too. A security breach in a Cloud or SaaS would bring not just financial, legal, reputational and regulatory risk to the vendor, but existential risk as well.*[9]

> **"In so many organizations, information security and disaster recovery are in different management chains, and the budgeted funds are not flowing in the direction of recovery."**

If that is what it takes to get to the beginning of the end, I am all for it.

Endnotes

[1] Ross, S., "The Train of Danger," *ISACA® Journal,* vol. 5, 2011, *www.isaca.org/archives/*. Myself included, no one who can write an article called "The Train of Danger" has any right to point fingers at others. But I shall point anyway.

[2] Churchill, W.; "The Bright Gleam of Victory," speech delivered to the Lord Mayor's Day Luncheon at the Mansion House, London, England, 10 November 1942. The exact quote is, "Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."

[3] IBM Security, *Reviewing a Year of Serious Data Breaches, Major Attacks and New Vulnerabilities*, USA, 2016, p. 5. IBM defines an attack as, "A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself."

[4] IBM, *2016 Ponemon Cost of Data Breach Study: Global Analysis*, 2016, p. 5, *www-03.ibm.com/security/data-breach/*

[5] Symantec, *2016 Internet Security Threat Report*, April 2016, p. 9, *https://www.symantec.com/security-center/threat-report*

[6] Ross, S., "Bear Acceptance," *ISACA Journal,* vol. 4, 2014, *www.isaca.org/archives*

[7] ISACA®, *Cybersecurity: What the Board of Directors Needs to Ask*, USA, 2014

[8] See the list of the top 500 in 2016 at *www.cybersecurityventures.com.*

[9] Cytryn, A., *et al*; "Hackers, Snoopers and Thieves: How to Handle the Latest Threats," *The Journal of Corporate Accounting and Finance*, July/August 2014, p. 49–50