information security matters

Challengeable Truths

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

It seems to me that everything I knew in my youth to be true has been overturned, refuted, disavowed or revised.[1] I have taken some of this rather hard, especially the news about Santa Claus. On the other hand, the process of learning to see the world in a different way has been a constant source of intellectual excitement my entire life. In information security, I have seen a vast revolution, from the days of "It cannot be done" to today's "It must be done." My enthusiasm about our profession has not only not abated, but it has increased enormously in the years—still just a few years—that the reality of the threat of cyberattacks has been recognized.

There were certain tenets that I absorbed as I learned my craft:

- Information resources are to be used by those authorized to do so.
- Encryption is the most effective way to protect information from misuse.

- Authenticated identity is the basis for access control.

These and many other verities are part of the tribal wisdom of the InfoSec clan; who am I to challenge them? Yet, since governments, criminal gangs and terrorists have taken to attacking the security of information systems, targeting individuals, corporations and governments, I have been forced to consider revising, if not abandoning, all that I have known to be true.

Authorization, Encryption and Identity

Is authorized use an immutable principle? This is a subject of hot dispute between the EU and the US. The European Court of Justice ruled in October 2015 that information owned by citizens in the EU was not safe from the unauthorized, prying eyes of security organizations in the US, especially the US National Security Agency (NSA). While the NSA has not officially said so, it would seem that its leaders feel that safety from terrorism overrides concerns about authorized use. Without expressing my opinion on the matter, I believe that information security professionals need either to relinquish the principle that only authorized use is permissible or defend it. It is no longer an unchallengeable truth.[2]

Much the same can be said about encryption. Is it a truly effective means of security if the bad guys can use it to subvert security itself? Many police agencies think it is not, while many in the information security field reject the argument for providing "back doors" to encryption schemes. I happen to think that back doors make it easier for crooks to outsmart the cops, but still the point of view of the US Federal Bureau of Investigation (FBI) and the intelligence community cannot just be dismissed out of hand.[3]

Access rights and privileges are accorded to individuals, presumably based on their job requirements. Increasingly, cyberattacks are being perpetrated not by the intrusion of malware, but by theft and misuse of the credentials of authorized users, especially those with privileged access. As noted by the US Federal Financial Institutions

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.*

Examination Council, "These attacks include theft of users' credentials—such as passwords, user names and e-mail addresses—and other forms of identification that customers, employees and third parties use to authenticate themselves to systems. Attacks also include theft of system credentials such as certificates."[4] In short, authenticated identity cannot always be trusted.

No Cyberrisk Assessments

All the foregoing is leading up to my assault on two chapters from the Book of Conventional Wisdom, beginning with: Risk assessments should *not* be performed as a component of cybersecurity.

Oh, yes, there are other books that insist on risk assessments, not least of which is the US National Institute of Standards and Technology (NIST) Cybersecurity Framework.[5] All the techniques that are discussed for performing a risk assessment are based on probability and the assumption that risk equals probability multiplied by impact.[6] This simplistic formula has been totally demolished by Nassim Nicholas Taleb's masterful book, *The Black Swan: The Impact of the Highly Improbable*.[7]

The argument for probability breaks down because it is highly improbable that any given organization will be struck by a cyberattacker today. Even over the span of 365 days, the probability would still be minute, so the annualized risk using the traditional formula is extremely low. Therefore, for many organizations, the result of performing a risk assessment would be to conclude that cyberattacks are not a threat to them and so nothing need be done.[8]

The determinant is not the probability of the threat of a cyberattack, but its credibility. If a threat is credible, management must do something about it, even if it is only informed acceptance of risk. Sadly, cyberattacks are a credible threat to all organizations. In this era, no one in the management of even a moderately large enterprise can say, "Oh, sure, we might be attacked, but oh, heck, let's take our chances."[9]

So if a risk assessment must be performed, here is my suggested process for doing so:

A. Are cyberattacks a credible risk? (Yes/No)

B. If yes, implement sufficient security controls.

C. If no, repeat step A.

System Crashes

Another revision of belief brought about by the advent of cyberthreats is: Treat all system failures as though they were caused by cyberattacks.

As long as there has been information technology, there have been system crashes. I am sure that Alan Turing[10] hung his head over his vacuum tubes wondering what went wrong. But even in wartime, I doubt that Turing ever thought that the cause of the failure was enemy attack. Even today, when a system goes belly-up, almost everyone thinks "bug" before they say, "Oh my, this must be a cyberattack."

> **"Organizations should react as though they were attacked until this can be disproven."**

This sort of thinking must stop. Instead of assuming that something benign has happened until it can be proven that the cause of a failure was a cyberattack, organizations should react as though they were attacked until this can be disproven. Yes, there will be many false alarms, but these should not add greatly to the mean time to repair. Whatever the cause, technicians must locate the flaw that caused the failure, but if they do not bring a mind-set that anticipates malign causation, it is less likely that they will see it even if it is there. The amount of time that it takes to eliminate a cyberattack as a cause of downtime is minimal compared with the time it takes to reverse the damage an actual attack might cause. (Perhaps military forces do assume they are under attack when systems go down. If it is permitted, I would like to hear from someone who can describe military thinking in this regard.)

Imperfect Assumptions

In the past few years, I have been addressing various aspects of cyberrisk more than any other topic. In part, this is because it is the greatest challenge of our time in the information security domain. World peace and climate change are weightier challenges, but we security professionals do not have much to contribute to resolving those. Cybersecurity, as I have previously said in this space, is above and beyond information security.[11]

> **"We should be open to revising what we think is true."**

Targeted attacks by powerful enemies are forcing us to reconsider almost everything we thought we knew about protecting information resources. The whole point of what I have written here is that we should be open to revising what we think is true because the bad guys are so good at finding the flaws in our shared, but imperfect assumptions.

Enjoying this article?

- **Learn more about, discuss and collaborate on cybersecurity in the Knowledge Center.** *www.isaca.org/topic-cybersecurity*

Endnotes

1 I have paraphrased—or frankly, stolen—this line from the play *Da* by the Irish playwright Hugh Leonard.

2 Farrell, Harry; "Safe Harbor and the NSA," *Washington Monthly*, 17 December, 2015, *www.washingtonmonthly.com/ten-miles-square/2015/12/safe_harbor_and_the_nsa059016.php#*

3 Sanger, David E.; "New Technologies Give Government Ample Means to Track Suspects, Study Finds," *The New York Times*, 31 January 2016, *www.nytimes.com/2016/02/01/us/politics/new-technologies-give-government-ample-means-to-track-suspects-study-finds.html*

4 Department of the Treasury, "Cyber Attacks Compromising Credentials Joint Statement," Office of the Comptroller of the Currency, 30 March 2015, USA, *www.occ.treas.gov/news-issuances/bulletins/2015/bulletin-2015-19.html*

5 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014, USA, p. 22-23, *www.nist.gov/cyberframework/*

6 Ross, S.; "Effective Techniques for Continuity Risk Management, Measurement," *TechTarget*, 2009, *http://searchcompliance.techtarget.com/tip/Effective-techniques-for-continuity-risk-management-measurement*

7 Taleb, N. N.; *The Black Swan: The Impact of the Highly Improbable*, Random House, USA, 2007

8 *Ibid.*, p. 40

9 Gustke, F.; "No Business Too Small to Be Hacked," *The New York Times*, 13 January 2016, *www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0*

10 Alan Turing, 1912-1954, was one of the 20th century's great geniuses. He conceptualized the computer as we know it in the 1930s and, during World War II, automated the breaking of the German Enigma code.

11 Ross, S.; "Frameworkers of the World, Unite, Part 2," *ISACA® Journal*, vol. 3, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*