# Information Security in Context

I do not believe in information security.

I support information security. I exhort organizations to implement and maintain information security. I have built my career around information security. But I do not believe in it. Belief is black or white. It admits no shades of grey. Security is not an absolute.

## Beliefs and Causes

I do have beliefs—religious, moral and political—which I have absolutely no intention of addressing in this *Journal* or any other public forum. In fact, they are not suited to discussion because, as beliefs, they are not subject to argument. One set of beliefs can only be confronted by another, not proven right or wrong. In the past, and even in the present, people have died for what they believe. I would like to think that I have the strength of character to die for my beliefs, but I am surely *not* prepared to die for the sake of secure information in any corporation or government agency.

I bring this up because I encounter many security professionals who act as though securing information is, for them, a holy endeavor. Unlike typical belief systems, security has no contradictory beliefs. No one is against security. (Of course, that is not literally true. There are some really bad people who are against security or, more precisely, they are against *your* security, but not their own.) In the absence of a counterargument, some security professionals I have met treat information security as a Cause, not as an attribute of information systems.

So what? Why is this bad? What is wrong with a little professional fervor? My concern is that such zeal leads to intransigence. It not only isolates the person, but also creates an atmosphere that runs counter to the establishment of an effective security culture within organizations. If security is portrayed as the One True Way, its proponents lose sight of the fact that others have different incentives, such as cost reduction, mission achievement and profit. It is not that security is inimical to these, but close-mindedness crowds out the ability to understand what drives other people. Thus, security receives resistance rather than an understanding that could lead people to accommodate security along with their own motivators.

## Context

This is not an argument in favor of compromise of the basic principles of information security. I prefer to think that it is recognition that security must be placed in context. The requirements for security differ in all sorts of organizations based on size, risk, resources and mission. So, for example, a company that makes household products simply does not have security needs as stringent as those of, for example, a large bank with billions that might be lost or a hospital where lives are at stake.

Moreover, information security is not a monolith. Data privacy is a major concern for those in health care or insurance, but less so for manufacturers, for whom trade secrets are a paramount issue. Fraud prevention is a focus of financial institutions, but less so for restauranteurs. So, someone pressing for across-the-board security can only be seen as foolish if he or she presses too hard.

This applies even in this age of cyberattacks. Much as I disdain those who dismiss this threat as not applying to their organizations,[1] it is true that some industries are more tempting targets than others. A small company that makes, say, plastic toys[2] is less likely to be attacked than a giant global brokerage firm. Once again, it is all a matter of context.

**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.

*http://bit.ly/2xmXwoM*

**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.

**Enjoying this article?**

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

## Persuasion, Not Proselytizing

In all organizations, information security needs advocates, not fanatics. No one in any information security department is going to achieve his/her goals acting alone. Security must be achieved through all the technicians and users in an organization. This calls for persuasion, not proselytizing. Security must be conveyed as a way of doing business that is beneficial for the organization, to be sure, but also for the individual. The inherent goodness of secure information resources must be demonstrated, not just presented as revealed truth. Information security professionals must be salespeople, teachers, leaders and exponents. I do not think the role of clergy fits very well.

I have heard too many security professionals complain that their management just does not "get it." Rarely have I heard someone say, "I did not do a good enough job explaining to them the benefits security would bring to them." I suggest that the cause of management recalcitrance is not opposition to security, but an ability to see a certain *degree* of security as acceptable. A *belief* in information security does not allow degrees; less than 100 percent means that there is a hole, which means that security is incomplete, which means that there is no security at all. Effectiveness arises from comprehension that security is a variable, not an absolute.

Conferences and seminars are wonderful for learning, but they are not ideal venues for listening to different perspectives about security. If everyone in the room is a fellow professional, there are not likely to be some more strongly in favor of secure information resources and others less so. There are shared assumptions and a common vocabulary that reinforce existing parochialisms. The presentations made are about how to make security better, not good enough. It is easy to see how context could be lost and zeal could take over. If that mind-set is carried back to the office, those not similarly passionate are more likely to be turned off than to be swept up in the resulting enthusiasm.

We who are in this profession "do" security all day. It is the reason why we come to work and many of us also take it home with us, in our heads if not our briefcases. Our objective is, or should be, not to get other people to do what we do, but rather to incorporate appropriate security into what they do all day long. They should make sales securely, balance the books securely, hire and fire securely. At best, we want them to influence others to work securely as well. But we will not get them to be fellow members of a campaign because it is not their fight.

> **"Our objective is, or should be, not to get other people to do what we do, but rather to incorporate appropriate security into what they do all day long."**

I have discussed the matter of security as a belief with colleagues and have drawn two reactions. Some treat me as an apostate for even raising the question. How could I abandon "the faith"? Others say that I am raising a straw man, that no one approaches information security as a religion or cause. In either case, I evidently have not explained my position well enough. By all means, be an advocate for information security. Be creative and influential in the communities of which you are a part. But temper the message so that information security is perceived as beneficial to the individual and the enterprise, not an unalloyed virtue unto itself.

## Endnotes

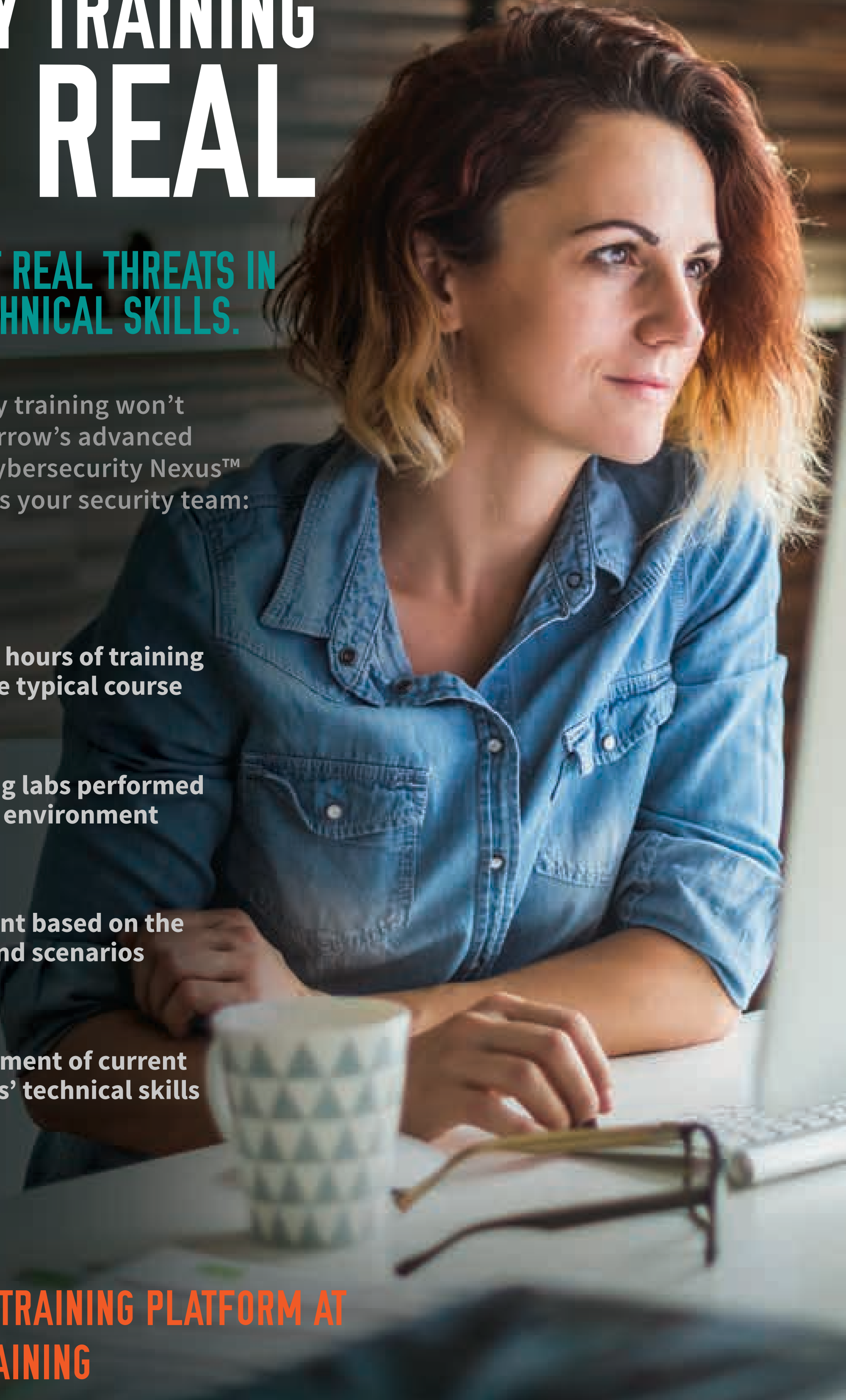
[1] Ross, S.; "Bear Acceptance," *ISACA® Journal*, vol. 4, 2014, *www.isaca.org/Journal/Pages/default.aspx*

[2] Gurtke, C.; "No Business Too Small to Be Hacked," *The New York Times*, 3 January 2016, *www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0*. The example was not chosen idly. In 2015, Rokenbok Education, a toymaker with seven employees, was the victim of not one, but two cyberattacks.

CSX

CYBERSECURITY NEXUS

# CYBER SECURITY TRAINING JUST GOT REAL



## NOW YOUR STAFF CAN COMBAT REAL THREATS IN REAL TIME TO BUILD REAL TECHNICAL SKILLS.

Yesterday's lecture-based cyber security training won't protect your organization against tomorrow's advanced cyberthreats. That's why ISACA's new Cybersecurity Nexus™ (CSX) Enterprise Training Platform offers your security team:

- On-demand access to 200+ hours of training for less than the cost of one typical course
- Practical, hands-on training labs performed in a live, dynamic network environment
- Continually updated content based on the latest real-world threats and scenarios
- Performance-based assessment of current and prospective employees' technical skills

**SCHEDULE A DEMO OF THE CSX TRAINING PLATFORM AT WWW.ISACA.ORG/CSXCYBERTRAINING**

ISACA®, the Cybersecurity Nexus™ (CSX) Mark, and ISACA's Cybersecurity Nexus™ (CSX) products, certifications, and services are not affiliated with CSX Corporation or its subsidiaries, including CSX Transportation, Inc.

ISACA®