information security matters

Chief Cyber Officer

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.

A few columns back,[1] I used the term "chief cyber officer." I had not thought of a position by that name until the moment I wrote it, but the term has stuck with me. I did a search on it at the time I was writing and found nothing.[2] It has rattled around my brain long enough. I think the time has come for me to address the need for such a position.

The Chief Information Security Officer and the Chief Cyber Officer

I can hear the rejoinder now: There is no need for a chief cyber officer because the chief information security officer (CISO) performs that function. Evidently Google thinks so as well. A search for "chief cyber officer" mostly brings up references to the CISO position. I maintain that there is a need for both, with, perhaps, a reporting relationship between them, with either a dotted or solid line. I see the chief cyber officer having a broader responsibility than information security as we have known it.

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.*

This is not meant as an indictment of the CISO function or of CISOs and other information security professionals. We must remember that the threat of cyberattacks is still new. The term "cybersecurity" (or "cyber security," if you prefer) did not enter the English language until early in this decade. The fact of cyberattacks is more important than the term. I cannot find references to deliberate, targeted, malicious attacks on information systems (my definition of cybersecurity) other than international espionage prior to the mid-2000s.[3] But information security professionals were hard at work well before then. The issues of the time were—and still are—viruses and worms, fraud, insider misuse, data leakage, encryption, and private key infrastructure, digital signatures and business continuity planning. These concerns may not have the sexiness of confronting foreign governments, terrorists and criminals, but they are still essential to the safe use of organizational and personal information resources. The mandate of a chief cyber officer would incorporate some aspects of information security, but would go beyond it.

Central to the differentiation of roles is my contention that information systems are not vulnerable to cyberattacks simply because they are poorly protected, but because they are poorly constructed.[4] Therefore, it follows that combatting these attacks goes beyond the purview of an information security department. What would a chief cyber officer do that a CISO is not doing?

Upgrading System Architectures

The underlying problem that enables attackers to get into information systems is that, historically, systems have "a hard crunchy outside and a soft chewy center."[5] If someone can penetrate the external barriers of firewalls and virus filters, he/she is free to roam around an organization's IT environment. Thus, the weakest point in a network defines the penetrability of the environment as a whole.

Solving this problem requires not only patching the holes, but reconstructing the entirety of an organization's systems architecture, not solely its

security architecture. This is a time-consuming, difficult and extremely expensive undertaking that must be carried out thoughtfully and carefully. With cybersecurity as the rationale for rebuilding a system architecture, it requires the knowledge, authority, and budget of an executive with a broad range of architectural skills, overseeing systems administrators, network engineers and database administrators, as well as information security specialists.

Re-architecting an IT environment is not going to be accomplished quickly. It must be rolled out over a period of years, perhaps many years. What is required at the outset is a reference architecture so that as systems are upgraded and changed, they can be accommodated to the intended to-be environment. This is a systems engineering mission, not one of information security alone.

Decision Making

There is, perhaps, no more crucial function for a chief cyber officer than recognizing that an attack is underway and initiating a response. It means that preventive systems have been breached and detective mechanisms have been activated, preferably at the time of the attack. This is not always the case. The Ponemon Institute reports, "Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify."[6]

Chief information officers (CIOs) often wait for business leadership to authorize the closure of a data center or a network. Cyberattacks demand rapid decisions. Therefore, a chief cyber officer must be empowered to make those decisions and be inoculated by the board of directors (BoD) from criticism by business managers.

Preparedness and Recovery

While a cyberattack is, *ipso facto*, a security incident, the response to it has to do with restoring servers and databases, not information security systems. These are involved only to the extent that any flaws that allowed an attack to proceed must be eradicated. The people who carry out the actual identification and removal of malware and the restoration of systems and data are those responsible for the systems and data—application developers, system administrators and database administrators (DBAs).

When and if an attack occurs, the response must be swift and disciplined. This requires ongoing training and drilling of and by the technical staff. A chief cyber officer would provide the leadership and oversight for what I call a CyberCERT,[7] which would be deployed at the first notice of a potential cyberattack. Many alarms will be false ones, so the expertise of the CyberCERT would be essential to identify a real attack and then move nimbly to respond to it.

"A chief cyber officer would provide the leadership and oversight for what I call a CyberCERT, which would be deployed at the first notice of a potential cyberattack."

Coordination

I see the chief cyber officer as an executive who draws on skills from many functions. These would surely include technical and information security specialties, but also those of legal, communications, training, physical security and risk management. The chief cyber officer would be the main channel between the BoD, the top tier of management and all the aforementioned specialists insofar as an organization's cybersecurity defenses are concerned. Externally, the chief cyber officer would represent a company or agency in dealings with police and security agencies, as well as with the media, customers and shareholders, when issues of cybersecurity arise.

Enjoying this article?

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

Politics

This will not be an easy job to fill or to execute. The effectiveness of a chief cyber officer position is dependent on the credibility of the threat of cyberattacks within an organization. Without that, there is no way for a chief cyber officer to demonstrate that he/she is actually achieving anything. Almost every day of the year there will be no cyberattacks, so there is no way to show progress, much less success. This has been a conundrum for CISOs for years, so it should not come as a surprise.

The relationship between the chief cyber officer and CISO could be fraught with jealousy, rivalry and internecine politics. It may be resolved, as I stated previously, by having one report to the other. However, that sets up a competition for limited funds allocated to information security that would only create its own political strife.

The potential for political infighting might be eliminated (or at least lessened) by appointing the person who is the CISO as the chief cyber officer. If such a position is established, moving the CISO into it is a logical career move. But this is predicated on the CISO having the skills and experience for the broader role as described. Many CISOs I know are well suited to be a chief cyber officer, but some do not have the verbal and interpersonal skills that would be essential for success in a coordinating role.

I do believe that there are CISOs and CIOs who are *de facto* chief cyber officers today. From the perspective of corporate governance, it is time to recognize that fact and set apart the cybersecurity function from that of building and implementing information security measures and running IT departments.

Endnotes

1 Ross, S.; "Cyber/Privacy," *ISACA® Journal*, vol. 1, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

2 As I write this, Google tells me that there are a few references to chief cybersecurity officer, which I will grant is pretty close to the same thing. But four references doth not a trend make.

3 The Merriam-Webster online dictionary cites the first use of the term in 1994, without attribution. I do not believe the term was in general use until around 2010. *www.merriam-webster.com/dictionary/cybersecurity*. The events of the mid-2000s that I refer to were attacks on the systems of the Estonian government and the theft of 45.7 million payment cards used by customers of US retailer TJX. See *NATO Review Magazine*, 2013, *www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm,* and Franscella, Joe; "Cybersecurity vs. Cyber Security: When, Why and How to Use the Term," Infosec Island, 17 July 2013, *www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html*

4 Ross, S.; "Microwave Software," *ISACA® Journal*, vol.1, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*

5 Not original to, but quoted from Kindervag, John; "Developing a Framework to Improve Critical Infrastructure Cybersecurity," National Institute of Science and Technology, USA, 8 April 2013, p. 3

6 IBM, Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," 27 May 2015, p. 3, *www-03.ibm.com/security/data-breach/*

7 Ross, S.; "CyberCERT," *ISACA® Journal*, vol. 5, 2014, *www.isaca.org/Journal/archives/2014/Volume-5/Pages/CyberCERT.aspx*