David Eduardo Acosta R., CISA, CISM, CRISC, BS 25999 LA, CCNA Security, CHFI Trainer, CISSP, PCI QSA, OPST, is an information security consultant. A lieutenant in the Colombian National Army's Professional Officers Reserve Corps, he works with Internet Security Auditors in Barcelona, Spain. He can be reached at *dacosta@ieee.org.*

Defensive Strategic Posture in the Field of Information Security

Invincibility is a matter of defense; vulnerability is a matter of attack.
—Sun Tzu

También disponible en español
www.isaca.org/jonline

The applicability of military thought to the field of information security has been the subject of discussion for a long time. From Sun Tzu's theories to Clausewitz's military doctrine, military concepts of strategy, operations and tactics have been compared to the activities involved in protecting information and managing information risk. In addition, these concepts have been applied effectively in areas as diverse as politics, marketing, business strategy and any scenario that entails the need to gain an advantage among players with conflicting interests.

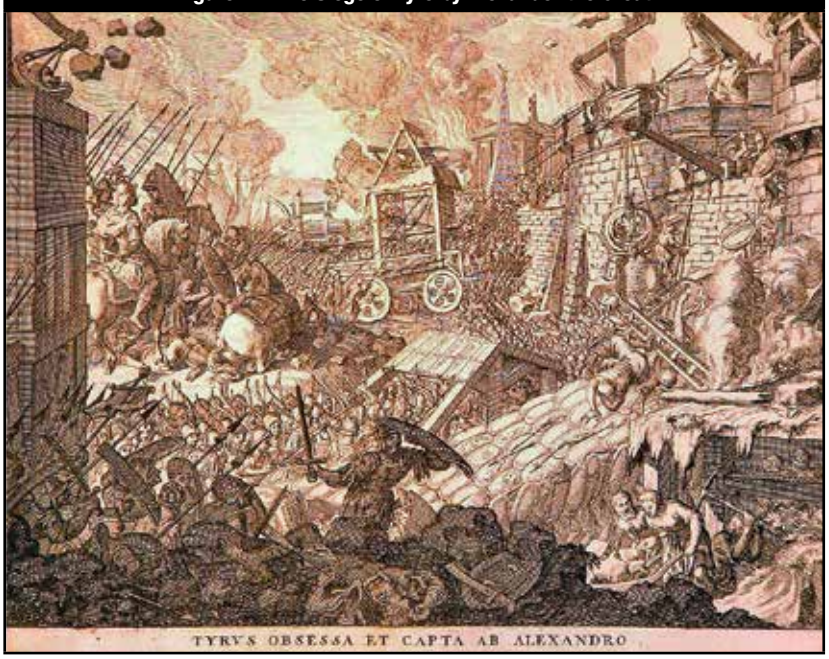
From a conflict-analysis perspective, any situation that disturbs a prior equilibrium of peace or *status quo* (in which needs are satisfied) always has two components: an offensive component and a defensive component. In precise terms, military strategy tells us how to use each component in specific situations, with the aim of achieving the objectives that led to the confrontation. Based on these strategies and tactics, as well as the defensive and offensive capabilities of the parties involved, the various conflicts can be classified in military terms as siege, trench warfare, conventional warfare, asymmetric warfare, terrorism and war of attrition. **Figure 1**, The Siege of Tyre by Alexander the Great (332 BC), depicted in a 1696 drawing, is a clear example of the use of defense and attack strategies by both sides.[1]

This article presents a review of the defensive strategic posture concept as it pertains to an organization's information security. In this context, the article explains why an organization must always adopt a defensive stance, as it is continually exposed to potential attacks, since it cannot engage in counteroffensive actions for legal reasons. The article rethinks the use of current defensive measures and their integration into a corporate strategy, with the aim of being able to react decisively to a potential attack.

DEFENSE AND OFFENSE IN THE CONTEXT OF ORGANIZATIONAL INFORMATION SECURITY

Any confrontation involves one party acting on the offensive and another acting on the defensive;

Figure 1—The Siege of Tyre by Alexander the Great



their roles may change over the course of the conflict. When acting on the offensive, a party always takes the initiative and engages in actions aimed at attacking the other party. When acting on the defensive, on the other hand, a party refrains from taking the initiative and waits for the attack in an effort to contain and repel it. When the party on the defensive finds the opportunity to attack, its strategy becomes one of *active defense*. Meanwhile, the attacking party—when attacked—converts its offense into a *passive offense*. In the words of Carl von Clausewitz, the defensive, "with the negative object, [is] the stronger [form]," and the offense, "with a positive object, is the weaker form."[2] Although numerous analyses have examined which of the two forms is more effective, what is certain is that, in general, the roles change as needs change.

Depending on the strategy, the operations and the tactics used by one party or the other, a conflict can result in one of four final states: win/lose, lose/lose, win/win or negotiation, in which the initial motivating factor plays a key role in the ultimate solution to the problem.

These concepts are easy to identify in any conflict in which the parties involved can (and generally should) act by combining defense and attack in a synchronized manner, as explained previously. Such actions are not foreign to the field of information technology, e.g., in the context of national cybersecurity. Hacking, electronic espionage and computer sabotage are among the newer components that have become part of the arsenal of weapons used to protect a nation's infrastructure. These concepts have encouraged the creation of a new generation of warfare: cyberwarfare or fourth-generation warfare, which involves the use of information operations (InfoOps). InfoOps include offensive and defensive cyber and computer actions intended to weaken and confuse the enemy and to protect the actor's own information resources, perhaps without any need for a direct confrontation (as was the case in the cyberattack against Estonia in 2007[3]). In fact, in the US, the White House published its *International Strategy for Cyberspace* in 2011,[4] and the European Union published its *Cyber Security Strategy* in February 2013.[5] These strategies describe the defensive and offensive actions to be taken in case of a potential cyberattack.

However, in the specific case of an organization, the scenario for responding to a potential attack is different. With the rise of the Internet, organizations today have adopted this medium as a basic channel for the exchange of information with outside parties. However, they are not certain when or how or why they may be attacked, and, thus, they are always in the position of awaiting attack. In fact, many computer security measures are based on the hypothetical premise of what can happen and what action will be taken. Clearly, the strategy has always tacitly been oriented toward defense. In many places, in fact, confusion between the terms "security" and "defense" persists. While security implies a state of exemption from dangers, damages or risks, defense refers to the actions taken to protect against such threats.[6]

For a company with a presence on a public data network, engaging in an offensive action in cyberspace is always in violation of the law and not politically correct, even if the action is taken as part of an *active defense*. In the face of such limitations, the traditional concepts of offense and defense cease to be valid in the context of organizational information security. The challenge takes the form of working with nothing more than a *defensive defense*, in which the objective is always to resist attack, with the aim of preserving the *status quo* and redirecting the offense back on the attacker by the very force of the circumstances. There is no counteroffensive, an attack is not initiated unilaterally, and the organization's own deployment is always defensive in nature and occurs within its own borders.

The limitation on offensive actions by the organization is well known to the potential cyberattacker. As a result, the attacker already knows beforehand that its attack will not be met with an active response and the organization's ability to respond offensively will be minimal or will depend on a third party (in this case, a police force or an investigative agency), facilitating the attack to some degree. The same offensive techniques employed by a cyberattacker can never be used, within legal limits, to respond to a cyberattack against an organization. If an organization used such techniques, it would be perpetrating the same crimes as those with which the attacker would be charged if it were prosecuted. This would not, under any circumstances, be part of a corporate policy.

A strategic posture constitutes the main stance in regard to a specific strategic objective. Traditionally, military planning opts for one of two strategic postures: an *offensive strategic posture* or a *defensive strategic posture*. Given the considerations and variables described previously, an organization must always design its information security strategy as a defensive strategic posture.

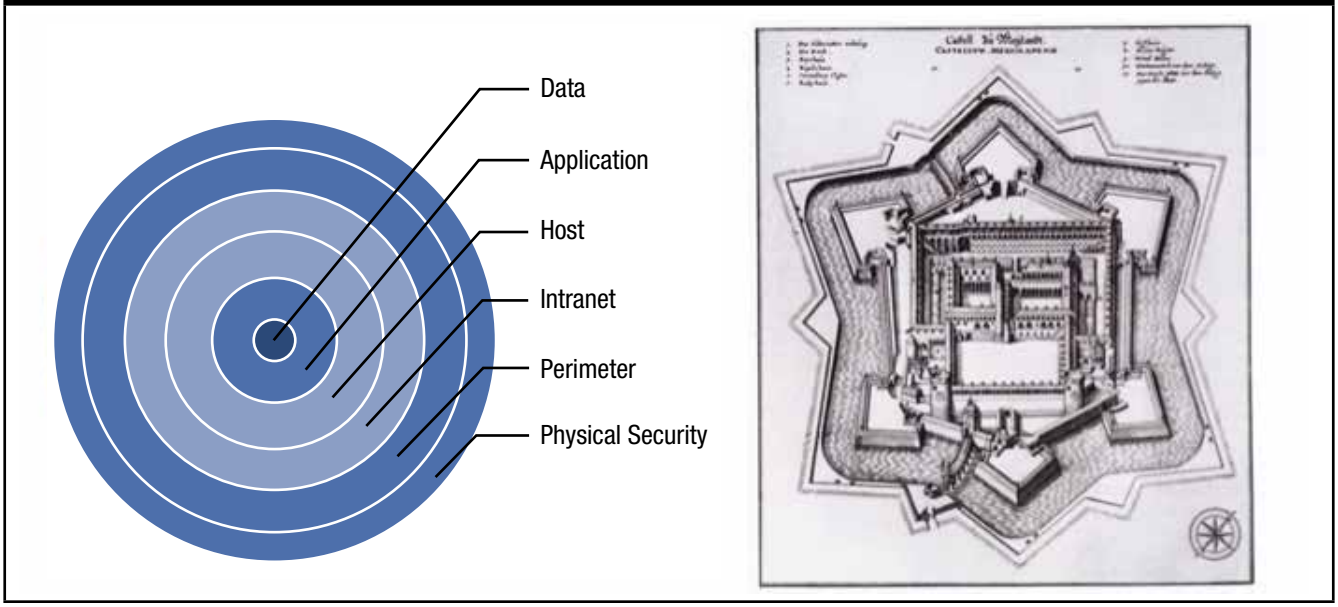
COOPERATIVE DEFENSE IN ORGANIZATIONAL INFORMATION SECURITY

The mere fact that a company has computer systems connected to the Internet poses a challenge for the security of the company. In practical terms, this situation could be viewed as equivalent to leaving a door open so that any ill-intentioned visitor can, at any time and any place, attack the infrastructure that supports these services. This fact leaves the organization in wait for a potential attack and at the mercy of multiple threats, without any possibility of engaging in a counteroffensive that might allow it to destabilize the attack. Unfortunately—and this is where the fundamental problem comes in—many people who are responsible for security view this state of affairs as a frustrating, negative situation, implying that any investment in defensive measures is not effective. The state of anticipation created by awaiting an attack at any time can become tiring, and it can make the most patient manager paranoid.

Firewalls, intrusion detection systems, intrusion prevention systems and disaster recovery plans, for example, are among the basic measures in a defensive posture to protect the organization's IT infrastructure. In many cases, however, because of lack of awareness and lack of a true systematic and comprehensive defense strategy, these measures are deployed independent of one another and on a reactive basis, or they simply are not in alignment with one another. As a result, the true value of the measures is not apparent, and it is not possible to evaluate the capacity to respond decisively to a potential attack. This fact is the Achilles' heel that results from chaotic use of defensive measures in a data network. In military terms, in this situation, tactical measures are deployed without having an overall strategy in common.

Proposing a *defensive strategic posture* as a key component of developing an organization's information security strategy should not be understood to mean adopting a pacifist attitude or disarming unilaterally. To the contrary, the model for the implementation of defensive measures must be planned and executed in such a manner that, in the event of any attack against the organization, the potential attacker is met with a decisive response, convincing him that he cannot achieve his objective and that the cost to him of waging the attack greatly exceeds the cost to the organization of defending itself. Therefore, the organization should expand its defensive measures, reflecting the investment that it would otherwise make in offensive measures. These defensive measures should be organized in a tactical manner, employing the *defense in depth* concept, in which there are various rings of security around the protected information. The structure is similar to that of a fortified building or a castle (**figure 2**).

Figure 2—Defense In Depth Model and Map of a Walled City



Specifically, models of secure network architecture based on defense in depth have been developed. These include McGladrey's ultra-secure model (Ultra-secure Network Architecture)[7] and Forrester's Zero Trust model.[8] These models establish guidelines for implementing measures that work together using the same model of layers and granular separation based on trust. They are clear examples of security strategies based on organized defense. No new components or unfamiliar technologies are added to the system. Everything lies in its organization, management and topology (with the latter being the distinguishing factor).

If an effective, unified defense capability is ensured, a potential advantage in the conflict is obtained. Carl Clausewitz gave an estimated relative advantage of three to one in favor of the defense in a conflict.[9] This means that an attacking force needs three units of attack against one unit of defense. In strategic terms, applying these theories, a defensive posture potentially would have a greater advantage in a conflict than an offensive posture. With this approach, the organization's security is ensured and the security of the networks to which it is connected is strengthened.

Also, in the context of cyberattacks, the laws and agencies that work to defend against such attacks are local and limited by the borders of each country. At present, there is no entity that would make it possible to manage a response at the global level, given the transnational nature of the Internet. As a result, an organization must depend to a great extent on itself for its own security. To support and supplement these actions, it is important to bolster the creation of mutually supportive defensive responses, known as *cooperative defens*e. For a cooperative defense security model to be effective, it is important for a company to begin by having its own credible capability in order to then present that capability to allies. Allies are understood as networks with which the company is connected (e.g., vendors, customers, subsidiaries) and which, at a given time, are able to support a defensive maneuver.

> "An organization must depend to a great extent on itself for its own security."

DEFINING AN EFFECTIVE DEFENSIVE STRATEGIC POSTURE

A strategy is a plan that is developed to attempt to achieve the strategic objectives that have been established. The objective of a defensive strategy in the context of information security is to ensure a continued existence on the net. This objective becomes a basic foundation that influences the organization's overall behavior and must be guided by a clear, comprehensive policy with support from management. It is important to bear in mind that in a defensive war, victory consists of systematically blocking the enemy's attacks.

A defensive strategic posture is comprised of two basic actions: waiting and reacting. These two actions should not be treated independently; they are mutually complementary. Waiting allows one to organize and prepare oneself effectively. As far as reacting is concerned, as the party on the offensive is carrying out its attacks, it gradually shows its strengths and weaknesses. These factors make it possible to provide feedback to the defensive strategy and prepare more effectively for a new attack.

To define a defensive strategy in the context of information security, one can use the same variables that are taken into account in guerrilla warfare, asymmetric warfare or terrorism. In these types of conflicts, forms of aggression are used that are similar to those involved in a cyberattack: sabotage; harassment of the target on its turf; use of irregular detachments with rapid, surprise attacks; secrecy; high mobility; temporary blockages of basic communication and supply channels; and seizure/theft of assets.

Based on these variables, it is possible to develop a series of defensive tactics and maneuvers such as those included in an anti-insurgency action plan. The term "anti-insurgency" is used rather than "counterinsurgency," since the latter includes offensive components that do not apply in an organizational context like the one described in this article. These analyses clearly lead to reexamining the classic view of theories of warfare in the cyber context: There is no readily apparent adversary, and the attacker does not wage its fight according to any rules or protocol, although the target of the attack does do so.

An anti-insurgency action plan is composed of four main components: prevention, deterrence, reaction and prediction. In a cyber context, since attackers rely on secrecy to carry out their actions, identification and prediction are the most complicated components to obtain. As a result, to implement a successful strategy, it is important to have some prior knowledge of the potential economic, political, social, ideological and psychological factors that may motivate the attacker. Prior intelligence actions should be used for this

purpose. Such intelligence is a fundamental part of threat identification, prevention, crisis management and tactics, and it may provide information about who, where, what, why, how and when. Since techniques such as penetration and infiltration are not practical ways generally to obtain information about cyberattackers (precisely because of their secrecy), this information must be approximated based on facts that can be obtained from past activities and information found in open sources. Generally, some of these offensive actions depend on publicity and propaganda.

Toward prevention, attempts are made to minimize the areas that attackers can exploit and a threat analysis is performed. These areas are not only technological. It is important to consider psychological, ideological, economic and other factors that may motivate an attacker to wage an escalating cyberoffensive against the organization. The effectiveness of good prevention depends on identifying these problems in a timely manner. An indispensable tool during the prevention phase is the analysis of historical information and past incidents, which can shed light on the motivations, tactics and maneuvers that the attacker may employ. Based on this analysis, actions involving deterrence, deception, attrition (depletion) and clearance, for example, should be defined.

In deterrence, the operational and tactical actions that define the organization's defensive and containment maneuvers in the event of a potential attack are planned and developed.

In reaction, the tactics and maneuvers that have been defined previously are put into operation based on the type of attack suffered. Some of the maneuvers to be executed include:[10]

- **Be on guard**—Be in a position that makes it possible to cover in time any potential vulnerabilities that the attacker may exploit.
- **Be clear**—Take actions aimed at drawing the offensive toward protected vulnerabilities.
- **Halt**—Protect a vulnerability that is under attack.
- **Dodge/elude**—Place the vulnerability that is the target of the attack in a position that is out of the attacker's reach.
- **Break/interrupt**—Stop, abandon a limited position.

One of the main objectives of these tactics is to exhaust the attacker—physically and in terms of morale—causing him/her to discard the idea of continuing with the attack. In addition, if some problem exists and the attacker manages to exploit a vulnerability, it is important not to play the insurgent's game. This game attempts to distort and confuse the defense in the face of an attack, provoking an emotional response rather than a rational one, which intensifies the problem. For this reason, it is important to establish crisis management for exceptional situations in which the organization is being subjected to an offensive, and calmly control the information that is made available to third parties in regard to the attack. Propaganda and publicity only strengthen the aggressor and may be one of the factors that motivated the attack; thus, the attacker would have achieved his objective, even if he does not carry the attack to its conclusion.

Finally, interaction with third parties (e.g., vendors, customers, investigative agencies) is part of a unified response—cooperative defense security. In this regard, coordinated offensive actions can be developed by agencies that are trained and authorized to do so.

Prediction is the feedback phase and allows the strategy to remain effective over time. Based on an analysis of the offensive actions against the organization and a new intelligence-gathering process, it is possible to predict an attacker's actions in an effort to strengthen weak points and optimize and adapt tactics and maneuvers.

To ensure that these strategies, as a whole, can be effective against a potential attack, it is important to conduct periodic self-attack exercises. A self-attack is a war game conducted by the organization with the aim of evaluating the defensive measures that have been implemented in a controlled scenario and under the same conditions that a potential attacker could experience, in order to detect problems and weaknesses in the theoretical underpinnings that have been defined. In this way, the system evaluates itself continuously and it is possible to incorporate new defensive measures in response to new offensive techniques.

THE "ARMS RACE" FOR A DEFENSIVE STRATEGIC POSTURE

From a military perspective, weapons are neither offensive nor defensive. Everything depends on the user's attitude. The same is true when it comes to information security: The tools are available, and depending on how they are used and the objective with which they are used, they may be employed to attack or to defend. When one of the parties to the conflict adds a new weapon to its defensive or offensive arsenal, the other party must act in kind to maintain the balance.

The idea of maintaining a defensive posture does not mean that the organization stays out of an arms race. The fact that an organization is defining a defense strategy may threaten or provoke the attacker. For this reason, as is the case with any strategy, it is important to maintain secrecy and discretion within the organization in regard to the strategy. Intelligence work, self-attack exercises and cooperative defense make it possible to keep the system and the strategy up to date as attackers make changes on the offensive side.

THE FUTURE OF DEFENSE STRATEGY IN INFORMATION SECURITY

As is the case with any strategy, the passage of time makes it necessary to reexamine actions on a small and large scale and to adapt to the constant changes in the circumstances. Failure to do so may mean ceasing to exist. In the context of information security, the organization's cyberborders are gradually beginning to blur because of the effects of technology. Cloud computing, managed services and interconnectivity with third parties, among other things, necessitate the design of shared defensive strategies that involve not just the organization, but also the other members of the ecosystem to which it belongs. If each component of this new system is aware of the need for a defensive strategic posture and takes steps to keep its defensive measures up to date, the sum total of these components will constitute an effective defensive block. This is true particularly when remembering that threats and vulnerabilities affecting one component automatically become threats to the other components, and as a result, the scope of the attack grows.

Coordinating unified policies, strategies, tactics and maneuvers, with the support of investigative agencies (external maneuvers), make it possible to develop decisive responses that serve to deter aggressors.

In a military context, one of the main challenges that a strictly defensive strategic posture (such as the one described in this article) can face is a siege or sustained attack. In an information security context, obviously, such an offensive could share similarities with a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack. In these types of attacks, the attacker attempts to take a system out of service through a large-scale offensive, overwhelming the target's defensive measures and often confusing the positions, not allowing the system to distinguish between an attack and an authorized activity.

One of the solutions to this problem is a cooperative defense security system, as discussed previously, in which the various parties affected by an attack coordinate with one another to respond defensively and control the attack (to the extent possible), attempting to minimize the damage. In addition, the multipresence factor should be considered. This entails the replication of content and services in various logical and physical locations, which allows the company to maintain its presence and operations in the event that one of its components is attacked.

CONCLUSION

The concepts of offense and defense do not belong exclusively to the military realm. For a long time, they have been applied in the sphere of information security (among many other spheres), and they are familiar (whether consciously or unconsciously) to those in charge of an organization's information security, given the continuous cyberthreats that are confronted daily. However, an organization that is the target of a cyberattack cannot engage in a counteroffensive to repel that attack, because of legal limitations. The organization is limited solely to defending itself, and, as a result, if no defined strategy is in place, the defensive component can become counterproductive.

Therefore, the intention—and, in the future, the task—is to step up the level of measures and response maneuvers that are now deployed (usually in a chaotic fashion) and to establish strategic defense criteria at the organization. These criteria allow the organization to act in a methodical, coordinated manner in the face of a potential attack, using and gradually strengthening its own defensive measures and becoming part of a global system of cooperative defense. This is a key objective to consider when implementing actions aimed at ensuring continued existence on the Internet.

REFERENCES

Aldao Zapiola, C.; *La negociación. Un enfoque transdisciplinario con específicas referencias a la negociación laboral [Negotiation: A Transdisciplinary Perspective With Specific References to Labor Negotiation]*, OIT/Cinterfor, Uruguay, 2009

Amidor, Y.; *Winning Counterinsurgency War: The Israeli Experience. Strategic Perspectives From the Jerusalem Center for Public Affairs*, 2010, p. 1-5

Foro Aviación Argentina [Argentina Aviation Forum], *La defensa no provocativa [Non-Provocative Defense]*, 2010, *www.aviacionargentina.net/foros/temas-de-defensa-generales.11/1626-la-defensa-no-provocativa.html*

US Department of the Army; *FMI 3-07.22 Counterinsurgency Operations*, USA, October 2006

Tzu, S.; *The Art of War, D.F. Anaya Editores*, Mexico, 2007

ENDNOTES

1 Image retrieved from *http://commons.wikimedia.org/wiki/File:Tyre_besieged_and_captured_by_Alexander_(1696).jpg*

2 Von Clausewitz, C.; *On War*, Spain, 1980

3 BBC News, *Estonia Hit by Moscow Cyber War*, 17 May 2007, *http://news.bbc.co.uk/2/hi/europe/6665145.stm*

4 The White House, *International Strategy for Cyberspace*, 1 July 2011, *www.whitehouse.gov*

5 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013, *http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security*

6 Vergara, E.; *Las diferencias conceptuales entre seguridad y defensa* [*The Conceptual Differences Between Security and Defense*] Instituto de estudios estratégicos de Buenos Aires [Buenos Aires Strategic Studies Institute], February 2009, *www.ieeba.com.ar*

7 McGladrey Consulting, *The Ultra-Secure Network Architecture*, 2013, *http://mcgladrey.com/Risk-Advisory-Services/The-UltraSecure-Network-Architecture*

8 Forrester Research, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, 17 September 2010, *www.forrester.com/rb/Research/no_more_chewy_centers_introducing_zero_trust/q/id/56682/t/2*

9 Ries, Al; Jack Trou; *Marketing Warfare, 2nd Edition*, McGraw-Hill, 2005

10 Beaufre, A.; *Introduction to Strategy, 3rd Edition*, Argentina, 1982

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

www.isaca.org