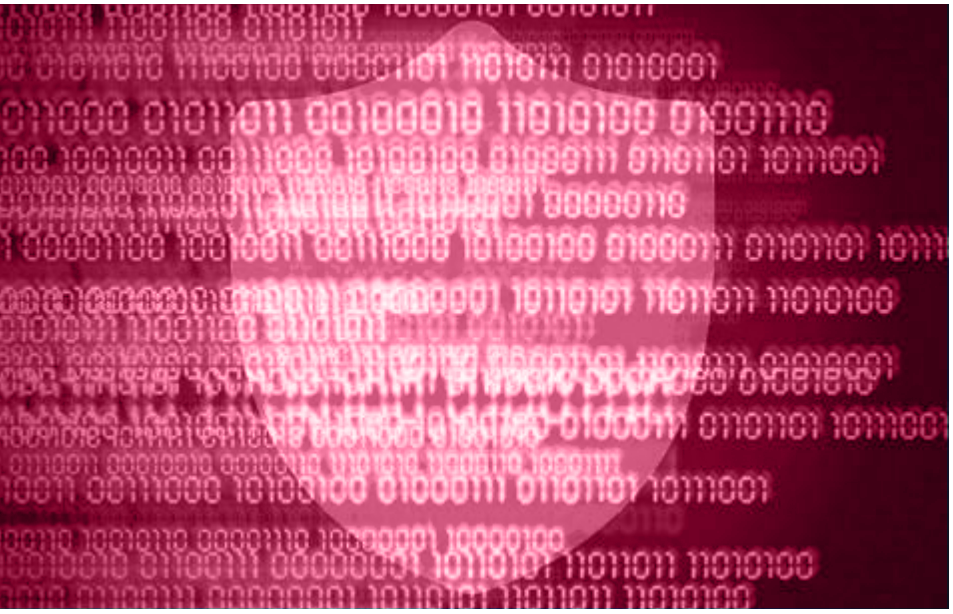
information security matters

Unsung Security Heroes

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.

Long ago and far away, I was the president of the EDP Auditors Association, which, some years later, changed its name to ISACA®. So here we are, 35 years after my term in office, and I marvel at what ISACA has become: 140,000 constituents in more than 200 chapters in 180 countries. One of the things I am most proud of in today's association is the breadth of its membership and the community it serves. Still having a base in IS/IT auditing, ISACA now encompasses consultants, educators, IS security professionals, risk professionals, chief information officers and internal auditors.[1]

It has been said that those who are professionally interested in the security and control of information systems, primarily IS auditors, have an adversarial relationship with the information technology function.[2] I do not think this is necessarily true or necessary at all. My experience, at least in the last decade or so, is that there are many in the ranks of IT professionals who are significant contributors to information security and who ought to be recognized as such.



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.*

Database Administrators

If there is any one attribute of information security that is universally recognized, it is control over access to data. According to one writer, "the database administrator (DBA) has three basic tasks. In decreasing order of importance, they are: protect the data, protect the data, and protect the data."[3] DBAs, or perhaps more specifically, data administrators, define the rules for data in the form of metadata. These set the policies for the use of data, in terms of the ownership of elements, usage by applications (and, by extension, people), and permissions to access, change or delete data.[4] All of that sounds very much like information security to me.

System Administrators

When a system has many users, someone must be responsible for installation, support and maintenance of that system. That person is known as a system administrator (sysadmin) and has wide-ranging authority for the contents, capabilities and performance of servers, network devices and other configuration items. It is understandable that those whose interests lie in information security should be wary of sysadmins, given the power they have over the storage and use of data. But sysadmins are, or should be, the first to know when a system acts strangely or fails.[5]

In my experience, sysadmins are very protective of their domains and very focused on the security and continued operations of the devices and software they support. So, despite their potential to undermine security, they are often the very ones who make sure security is working.

Disaster Recovery Planners

Sometimes, despite all security measures, systems fail. When the cause is physical in nature, we call it a disaster, and when a disaster befalls a data center,

it is the disaster recovery planner who should have developed the procedures for restoring operations, usually at an alternate location. This person must have a broad understanding of infrastructure and applications in order to effectuate recovery within management's tolerance for downtime and data loss.

> **"In and of itself, disaster recovery is an aspect of information security."**

In and of itself, disaster recovery is an aspect of information security. Moreover, disaster recovery planners need to maintain access control, intrusion detection and other safeguards in the restored environment at the same level as in normal operations. Consequently, they have many attributes that make them participants in the management of information security.

Business Continuity Managers

Closely aligned (and allied) with disaster recovery planners are business continuity planners. Where the former prepare for recovery of IT operations, the latter ensure that business activities can continue at some acceptable level while systems are down. In instances in which no downtime is acceptable from a business perspective, the business continuity manager becomes the advocate for the end users in dealing with IT management.

Some would question whether business continuity management is an information security function at all. For many years, the basic global security standard, ISO 27001, defined business continuity management as a component of security. In the 2013 version, with the publication of ISO 22301 as a parallel business continuity management standard, the focus has shifted to maintaining security in recovery situations.[6]

Procurement Personnel

In our interconnected age, it is widely recognized that the security and recoverability of third parties are critical elements of information security. When systems in the form of products and services are purchased, it should be clear that the requirements for security are as high as those for systems developed internally— perhaps more so, inasmuch as the acquiring organization has little or no control over the vendor's development practices.

The person who is best positioned to insist on built-in security is the procurement manager. I will leave it to a future article to consider how this person, presumably without deep IT or security skills, might understand an organization's security requirements or recognize whether or not they are met. Nonetheless, procurement managers can be instrumental in achieving a consistent level of security across an enterprise.

Project Managers

Even if a system, whether acquired or developed internally, has the best security controls, those controls may be meaningless if not implemented properly. Sizable projects—and implementing systems is almost always a significant project—require capable project managers. It is these project managers who ensure that systems are put in place the right way, using the right methods and controls, meeting the owners' requirements, and, oh yes, on time and within budget. Somewhere in their mandate, project managers must make sure that security has been properly embedded in the systems.

Project managers should have the knowledge and skills to relate to all the security requirements of the system project they are overseeing. This requires an understanding of how the system in question meets those requirements and how the way that a system is implemented supports (or fails to support)

Enjoying this article?

- **Learn more about, discuss and collaborate on business continuity/ disaster recovery planning in the Knowledge Center.** *www.isaca.org/topic-business-continuity-disaster-recovery-planning*

security. Project managers must think broadly, considering not only the security of the subject system, but all the other systems running in the same environment, which, increasingly, means the entire application and infrastructure portfolio.

That is why those of us who do have some depth of information security knowledge must work with project managers and all the other professionals mentioned above, with a mutually respectful (and nonadversarial) relationship. Bringing all the skills together can only enhance an organization's security and the quality of the overall IT environment. So if you want to do something to foster information security, consider taking a project manager to lunch. And next week, a DBA. And after that, a sysadmin…

Who knows, maybe you can convince them to join ISACA.

Endnotes

1 ISACA, Membership, Guidance and Certification for IT Professionals, *www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx*

2 Singleton, T.; "Why Everyone Dislikes the IT Auditor and How to Change It," *ISACA® Journal*, vol. 1, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

3 Watkins, B.; "What Does a DBA Do All Day?," *Enterprise Cloud*, 26 June 2008, reprinted in *Tech Republic*, *www.techrepublic.com/blog/the-enterprise-cloud/what-does-a-dba-do-all-day/*

4 Cox, T. B.; "The Role of the Database Administrator," *Computer Weekly*, March 2000, *www.computerweekly.com/feature/White-Paper-The-role-of-the-database-administrator*

5 Gite, V.; "What Is the Role of the System Administrator?," nixCraft, 20 February 2006, *www.cyberciti.biz/faq/what-is-the-role-of-the-system-administrator/*

6 Verry, J.; "Is ISO 27001:2013 Clarification of Business Continuity Driving ISO 22301 Certification?," *PivotPoint Security*, 14 November 2013, *www.pivotpointsecurity.com/blog/iso-27001-2013-business-continuity-iso-22301/*