TRAINA & ASSOCIATES
A CAPINCROUSE COMPANY

4 Steps to a Solid User Administration Process

By Kamilla Ben, Senior and Lisa Traina, Partner, Traina & Associates

Although it may seem like a small detail in the grand scheme of cybersecurity, a good user administration process plays an important role. This means establishing a thoughtful process for controlling administrative access to applications and systems.

Many organizations feel that employees obviously need access, and it should just be given to them. But you should consider necessity in all instances and for all individuals. Taking some basic steps will help your organization create a solid user administration process and reduce your organization's risk of a breach.

1. Know your applications and risk-rate them.

You need to know which applications your organization uses and what information they store before you can identify the risks inherent within your organization's daily activity. Ask:

- What applications do we use?
- What type of information do these applications hold?
- What level of risk is associated with the information (e.g., is it or could it be considered confidential)?
- What potential for exposure exists? What are the potential repercussions for your organization if the information is exposed?

This information may be more difficult to identify if your organization has a decentralized environment for user management. Consider asking individual employees or departments what applications they use. Many organizations identify applications they didn't know were in use.

2. Categorize your applications based on criticality to determine your highest-risk applications.

High-risk applications are those that contain sensitive or potentially sensitive information. This includes information considered proprietary to your organization or to others. Another factor that can increase an application's risk is whether it can be accessed from the public Internet, as externally accessible systems and applications increase the risk of unauthorized access if not properly secured. These applications should have strong user access controls in place.

3. Establish a formal user administration process.

The goal of user administration is to ensure that access remains properly restricted throughout an employee's time at the organization. Consider these three phases of the employee life cycle:

1. Hire – How do we ensure an employee receives only the access they need?
2. Job changes – If an employee's job function changes, do we ensure removal of access that is no longer required?
3. Termination or resignation – Do we ensure access rights are canceled in a timely manner when an employee leaves?

Then for each phase in the employee life cycle, ask:

- How will access be granted?
- Will access rights be based on job position, or on an individual's unique role?
- Can we establish a profile that gives a user access to the needed areas only?
- Which individuals or roles require administrative functions? Administrative access should be granted on a limited basis.

In a centralized environment, application administration is the responsibility of one area or department, typically the IT department.

In a decentralized environment, responsibility for user access management is delegated to the departments that use the applications. This does not remove management's responsibility to know which applications are in use and who is using them, and poor management can often heighten the risk of a breach. However, as long as you formally define the process, a decentralized

environment can achieve the same results for user administration.

4. Audit the process you have in place.

It's not enough to establish baselines and policies. Your organization needs to evaluate them periodically to ensure they are effective, and working and used as intended.

- **Implement a regular review of systems**. At least annually, review all users on each application to ensure that they still need access to the application and still require their existing level of access. You should review high-risk systems more frequently, such as quarterly. The reviews should be documented and approved, especially if a decentralized system in place.

  During this review, verify that terminated employees have been removed, access rights and administrative functions are still warranted, and service, system level, and vendor accounts are still required. Some applications allow you to create reports showing the last login date for accounts. This could help you identify accounts that are no longer required.

- **Implement alerting and log review**. Can you configure applications and systems so that appropriate personnel receive an email alert any time a change is made or access is adjusted? Consider reviewing a change log weekly to identify changes that should not have been made. This type of ongoing monitoring can help make your overall user access management process more effective.

Implementation and follow through on these steps will help your organization establish a solid user administration process and maintain clean user access for all your applications.

About the Authors

Kamilla Ben, Senior
Traina & Associates, a CapinCrouse Company
kben@capincrouse.com
o 817.328.6510

Kamilla joined CapinCrouse in 2012 after six years in an accounting and finance role with a not-for-profit organization in Colorado Springs. She provides audit, review, compilation, tax, and consulting services to a range of nonprofit clients.

Lisa Traina, Partner
Traina & Associates, a CapinCrouse Company
ltraina@capincrouse.com
o 225.308.1825

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017.

About Traina & Associates*

Traina & Associates, a CapinCrouse company, has been providing information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations since 1999. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at trainaassociates.com.

*Traina & Associates is an authorized trade name of Capin Technology LLC, a subsidiary of Capin Crouse LLP.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.