Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

technology may have been offering self-service options to extend back office functionality. Electronic invoicing and collections are two early examples that date back to the ...

Jun. 19, 2018

In 2018, the year of artificial intelligence, internet of things, blockchain, and big data, it is safe to say more and more companies are emerging to be technology companies. In the last year, a lot of attention has been placed on how automotive companies such as Ford and General Motors are positioning themselves as

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Banking Group's geographies." Verticals such as healthcare, education, media and many others now must address technological changes more than ever and position their investments in technology as differentiators.

Technology and CPA Firms

CPA firms are also once again changing. For many, the first customer facing technology may have been offering self-service options to extend back office functionality. Electronic invoicing and collections are two early examples that date back to the 1990s or earlier. As time moved on, other parts of the business, particularly those related to engagement delivery, also began to leverage technology. In the 2000s, firms began using file sharing services and central repositories such as Microsoft SharePoint to exchange data with clients. Most firms purchased commercial-off-the-shelf (COTS) products as they did not have many, if any, developers on staff. Today, firms have a plethora of on-premise and cloud-based offerings available and if none of them meet requirements, the potential to develop something in-house is readily available. These new solutions also require firms to think about security more than ever before.

Large Firms and the Cobbler's Children

Many CPA firms, particularly larger firms, offer technology related advisory and consulting services, including developing software for their clients. However, they also need to innovate and leverage technology to improve the quality of their own offerings, be it tax, audit or advisory. These firms often have staff with the knowledge to adequately secure their own environment; however, they rarely work with internal initiatives. The problem is the work performed for the firm's external clients are revenue generating, while securing internal systems yields no revenue, or is seen as taking away revenue due to the opportunity cost.

Smaller Firms and Knowledge Gap

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Whether a firm decides to buy or build there are many security considerations to address. For firms on a tight time frame or need a concise reference, the following checklist covers fifteen of the most common controls that should be considered when deploying a new technology.

1	Authentication	Are users of the system required to use strong authen
2	Authorization	Have permissions and roles been appropriately defin implemented?
3	Backup	Are all critical systems routinely backed up and are tl backups tested?
4	Change Management	Does a formally documented process exist to track ar changes?
5	Continuous Monitoring	Is a process in place to continually evaluate the secu environment?
6	Data Classification	Has the data being used by the system been categoriz inventoried?
7	Encryption	Is the data secure while in transit and at rest?
8	Incident Response	Are people, processes and technologies in place to ad security breach?

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

		basis?
12	Physical Access	Is physical access to the system adequately restricted
13	Policies & Procedures	Do documented security policies and procedures exis environment?
14	Service Level Agreements	Have service level agreements been established with and/or for clients?
15	Third parties	Are all third-party interconnections known and bee documented?

Preparing for the Next Project

In addition to the determining what things should be evaluated when implementing a new technology, firms need to understand when to begin asking these questions. It is paramount that an understanding of the controls in place occurs as early as in the system development life cycle (SDLC) as possible, preferably in the requirements gathering and planning phases. While identifying gaps later in the SDLC is better than not knowing them at all, the cost to remediate gaps increases greatly went they are identified later in the project.

============

Matt Wilgus is a Practice Director at Schellman & Company, Inc., where he leads the Threat and Vulnerability Assessment offerings. In this role he heads the delivery of

Schellman's penetration testing services related to FedRAMP and PCI assessments, as

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved