

2024 CYBERSECURITY EXECUTIVE BRIEF FOR ACCOUNTANTS

The cybersecurity landscape continues to evolve into 2024 and beyond. As it does, accountants and other financial professionals must stay apprised of developments that could affect the security and compliance of their work – and even put their businesses at risk.

In this Cybersecurity Executive Brief for Accountants, you'll learn about:

- **Cloud inevitability** –and a silver lining
- **Ongoing endpoint security concerns**
- The social and reputational risks of a breach
- **Increasingly complex partner requirements** (such as cybersecurity questionnaires)
- Why **awareness training** is the most important tactic of all
- The failures of IT services taking a **reactive, not proactive, approach**





Cloud Inevitability: Accounting Applications Increasingly Moving to the Cloud

One of the clearest trends in cybersecurity that's relevant to accountants and accounting departments is **the inevitability of the cloud**. More and more accounting applications are allocating more and more of their resources to their cloud product, not their desktop, server, or on-premises version.

And that's assuming they have a non-cloud product at all: **some newer players never had an on-premises version to begin with.**

Take Quickbooks for example: for many years, Quickbooks offered a cloud version that was, at best, a slimmed-down version of the "full Quickbooks experience." If you wanted that full experience, you had no choice but to use the desktop or server version.

That's no longer the state of the landscape. Intuit has continued to update and innovate in its cloud product so that today, switching from their legacy platform to their cloud platform is **seamless** for many accountants.

And switching isn't really optional, at least not for long: Intuit has been fairly open about the fact that they've poured their development efforts into the cloud product. The company doesn't seem to be preparing any new major updates to the desktop application or the server version. **Within a couple of years, it's quite possible that Quickbooks will be cloud-only.**





A Cloud Silver Lining

Many businesses and accountants who have not yet switched to the cloud may find this cloud inevitability quite frustrating. **Change is disruptive, after all.**

But there's a silver lining to this cloud, and it's a big one: cybersecurity itself.

With the on-premises/server/desktop versions of most accounting software, the security of the application is almost entirely the responsibility of the business and its users. **Put simply, if the bad guys hack your servers, no one at Intuit or other vendors is responsible – and no one there will help you fix the problem.**

In this scenario, if a business doesn't have the necessary safeguards in place, they could put their business's reputation – if not its entire existence – at risk.

But the cloud version of that same piece of accounting software is different: it runs on the software vendor's servers, not yours.

The security safeguards a corporation like Intuit (**and its cloud hosting provider**) puts into place will undoubtedly be more stringent than what most small businesses are capable of establishing.

So, to sum up: **by switching to the cloud, businesses offload significant amounts of cybersecurity risk**, relying on (much larger) software vendors and cloud service providers to maintain that security at a level that would be unsustainable for nearly any small business.



Endpoint Security an Ongoing Concern

With a sudden, aggressive shift to remote and hybrid work now a few years in the rearview mirror, businesses continue to grapple with the ramifications of this new way of working.

Far more employees who can work remotely are doing so, at least some of the time. They tend to access their work from whatever device they want to use, if allowed that freedom.

The challenge at this stage has shifted from yes-no decisions about remote work and boardroom discussions of return-to-work policies.

Now the conversation (at least the one that should be taking place) is on how to navigate this new way to work safely and securely.

Endpoint security – that is, the security of whatever devices employees are using to access business resources – is an ongoing concern for remote, hybrid, and distributed businesses.

Endpoint management software and strategy (along with mobile device management, or MDM) is the mechanism that most SMBs turn to for this piece of the cybersecurity puzzle. It's not foolproof and it's not one-size-fits-all: for example, some organizations can allow more liberal access from unmanaged mobile devices, while others shouldn't.

There are also numerous ways to handle authentication, each with its own set of pros and cons. Some are more secure but harder to use; others solve the ease-of-use equation but are comparatively less secure.

Working with a managed IT partner that understands endpoint security and MDM – the way they work today, not five years ago – is a key strategy for most SMBs.



Social Proof: A Double-Edged Sword

Businesses often talk about social proof in a marketing context, where customer testimonials or online reviews can make a real difference in new customers' decision-making.

Social proof remains as important as ever in this way, as consumers (and individual decision-makers at businesses) tend to trust the people they know.

However, social proof can be a double-edged sword: just as positive reviews can draw in new business, negative publicity can do damage at an unprecedented scale in this social media age.

Clients (and would-be clients) care more than ever about image and reputation. A cybersecurity breach – especially one involving or originating in accounting – threatens to damage or even destroy a business given the rate the news spreads on social media and in business networks.

Think of it this way: **A ransomware attack costs far more than the payment demanded by the attacker. The costs in lost reputation – and lost business – could far exceed whatever the attacker demanded.**



Partner Complexity: Cybersecurity Audits and Questionnaires

The way we work continues to grow more complex as businesses add vendors (or become vendors themselves to other businesses). Digitally connected systems are a necessity for these partnerships to work, but every point of digital connection could be a threat, a potential vulnerability to be exploited.

To stay safe and protected in this ecosystem, many partners and vendors are now requiring the completion of a cybersecurity questionnaire, survey, or audit before agreeing to do business together.

Organizations are beginning to demand that their partners have a baseline cybersecurity standard. This is a net good for the world of connected businesses (because breaches hurt everyone), but it does create more work and a heavier administrative burden.

More and more, we see organizations that don't have a managed IT partner falling behind in this area. Completing these questionnaires, which can be significant in complexity and scope, amounts to more work than anyone has time to do, and it requires maintaining a level of IT preparedness that organizations cannot maintain.

Often we see a firm reach out in desperation to an IT services partner to take on this responsibility on a crisis timeline, **leading the business to rush their due diligence and pick from only those managed IT firms desperate enough for new business to take on the rushed project.**

We see a better approach here: **take the time now to find the right managed services partner so that service contracts are already in place the next time you face a complex cybersecurity questionnaire.**





Cybersecurity Awareness Training Essential

Cybersecurity awareness training is an absolute requirement for all users at a financial firm. This is because people are always the weakest link: your biggest threat could be the unwitting actions of your own team members (falling prey to a phishing email or a phone scammer or any of a host of other cyber threats).

Many of the tactics cybercriminals use are relatively easy to spot – if users know what to watch for. This is the main benefit of cybersecurity awareness training. **It isn't a fluff service and should not be a recommendation, but a requirement.**

A good rule of thumb is to add cybersecurity awareness training into **new user onboarding** (e.g., as cybersecurity modules alongside other onboarding modules) and require **annual training** (provided by IT) every year at the same time.

Compliance can be a concern, so consider providing incentives for completing or disciplinary action for failing to complete training.



“Call When You Need” IT Approach No Longer Sufficient

As organizations’ IT ecosystems continue growing more complex, a new attitude toward IT support becomes necessary.

An existing approach to managed IT services takes a hands-off stance, saying in effect, “We’re here when you need us – just give us a call.”

But “give us a call when something breaks” is no longer sufficient, plain and simple.

Yes, this approach appears cheaper overall (in terms of a monthly or yearly service agreement). But it leaves holes in nearly every layer of an organization’s IT and cybersecurity posture.

Consider these negative effects of a hands-off, reactive IT approach:

- No active monitoring of cybersecurity threats and network intrusions
- No ongoing master plan for updating technology and software
- No active managing of devices
- No focus on keeping cybersecurity policy and protections current

In the end, organizations taking a “call when you need us” approach expose themselves to huge risks, especially related to cybersecurity.


What’s needed instead is a **proactive partner**, a managed IT services provider that guides you in IT planning and execution and stays with you every step of the way.

Reach out today if your business is still looking for the right fit!



 1.844.XENTRIC

 hello@xentric.com

 xentric.com