

Top 10 IT issues for small businesses or not-for-profits

Sandra Johnson, CISA, Manager, Baker Tilly Virchow Krause, LLP

August 30, 2010

Before we discuss the top 10 IT issues at small businesses or not-for-profits, we should establish that many of these issues come about from operational and economic considerations and to what extent IT plays in their businesses. If IT is integral to the success of your business, then you should strongly consider following IT General Controls best practices and make annual progress towards that goal.

In my field of expertise I see and hear from many clients that their financial application is a necessary evil for financial reporting. They don't see the importance of having it follow best practices for IT General Controls. While I don't know if financial applications are evil, the applications do need to be updated, controlled and monitored by management. To that point, most companies agree. However, having to perform work around the IT environment causes them great distress. Here is where the operation, economic or the level of importance comes back in our discussion.

The operational push backs usually go something like this:

1. "Server and financial application updates are applied so infrequently that we apply them directly to the server or personal computer without first testing them."
2. "We have so few financial application users that we see no need to monitor transactional history or logical access controls."
3. "We run backups nightly but no one checks the backups for data integrity or performs a backup restore test annually."

Economic push backs:

1. "We have such a small office staff that we just don't have time to perform these tasks."
2. "We just don't have the money to fix these issues in this year's budget and it will take board approval for next year's budget."

While I sympathize with these clients, I still have to stress is that if your application and network environment is not following IT General Controls best practices you may have a whole host of other issues down the road. We've all heard of financial fraud, but what about the growing number of data fraud cases that are being perpetrated on individuals and businesses today? Before you say we're small (i.e. \$5 million, \$20 million or \$100 million or less it's all relative to your line of thinking) or the notion that we fly under the radar so we feel the business has little to worry about, think clearly about the inherent risks surrounding any amount of money. Think of all the stories about fraud that you have heard where the culprit "was the last person we ever would have expected". There is another thought that states that ignorance is bliss and because someone doesn't that much about the application, they can't hurt you. Having a few or some IT controls in place is not a level of protection that should be relied upon..

The size of the business is not what makes the business a target. It's that someone can take without much effort either internally or externally. Let's face it – a big company may pose a great target, but they also have large IT Departments protecting them or working towards that goal. Small businesses, however, frequently run by the "seat of their pants" so to speak.

The Baker Tilly Virchow Krause, LLP emphasis on industry specialization prepares us to offer honest, informed ideas and act decisively.

It is not a matter of why your business will be targeted but when.

Putting in the proper IT or financial controls can help you to prevent, identify or at least detect the theft afterwards. The difficult question to have to respond to is why if there are no IT controls in place to detect a data breach or event that has occurred. The operational and economic costs of an undetected data theft may far greater exceed the money needed to establish the proper IT controls early on. There is not a business today that wants to be publicly tied to a data theft or financial fraud, but it stills happens daily. The costs of retaining your existing or prospective clients, business partners and employees maybe so costly that there's no business left to save once the damage has been made public.

The top 10 IT client controls I see lacking on regular basis:

1. Change or Patch Management
2. Logical access authentication
3. Strong network and financial application password and lockout settings
4. Logical access user request process
5. Administrator or Super User roles and responsibilities
6. Logical access reviews
7. Internal and external security monitoring
8. Physical access to IT environment
9. Vendor management
10. Backup or computer operations

Some of the reasons why a business owner should care about these may not be obvious. Let's walk through some of the basics.

1. Change or Patch Management processes and controls should be documented so that management has a way to determine which updates or patches should be accepted or rejected. Some changes may cause system disruptions or network failures upon installation to your operational environment. No two IT environments are exactly alike so there's always a small gamble taking place when you apply updates directly to the production environment at the server or application level. Another possibility is that in the event of a disaster or system melt down, you may want to know what platform, updates and patches have been applied so you can reconfigure the repaired or new piece of equipment quickly.
2. Logical access authentication means having no two users accessing the same user id, generic, temporary or system ids on the network or the financial application to login. Each user should be uniquely identified so no one hides behind a veil of anonymity or uncertainty as to who performed or removed a transaction. There's also the tendency for generic user ids and passwords to leak out; allowing more users know about them and potentially use them inappropriately or maliciously.
3. Strong network and financial application password and lockout settings mean having password aging (90 day maximum), history checking, complexity (alpha numeric characters), and lockout settings (five attempts for thirty-minute lockout without IT intervention). Now, I know most of you will tell me this will be far too disruptive or cause office pandemonium if you enforce these settings but I assure you it will not. While there will be some users that will complain, the requirement to use strong passwords and to renew them periodically is not unusual in today's market place. How one tracks or maintains their passwords is the key.

4. Logical access request process for a small or large company should be documented so you know how much access has been requested and approved for each user. With staffing and management turnover, it can become the norm to “clone” users rather than defining an application role or level of access needed based upon their job description. Too much access to a variety of roles or data can be very costly if there’s data disruption due to a training issue or malicious activity occurring. The use of standardized roles will also become clearer when you try to perform user access reviews.
5. Administrator or Super User roles and responsibilities should allow IT users the ability to support the network or application environments, but they do not need have the keys to the kingdom or otherworldly powers. Being the Domain, Database or Application Administrator does not require IT administrator user’s access to root, system fire call ids or shared system user ids for their day to day responsibilities. Admin or Super Users should have unique user ids for their normal job responsibilities and the use of root or system ids should be used sparingly and tracked by management for necessity and not for the ease of doing their normal job responsibilities.
6. Logical access reviews require management to know what access by has been requested individual user or user role, approved, set up on the network and financial application. The primary issue is that without a user request processes in place, performing user review controls are difficult at best, and harder for management to implement later. User access reviews require business or application owners to understand how the network and application access setup and determine if each user has the appropriate amount of access. Too much access can allow an inexperienced user to execute financial transactions wherein they may not understand all the ramifications.
7. Internal and External security monitoring go hand in hand with the other access controls. Informed users will know that all transactions can be monitoring internally and externally through the use of auditing logs or security monitoring tools. Users are far less likely to perform fraudulent transactions or dump data to an external source if what they’re doing is being monitored or could be identified later through the review of security audit logs.
8. Physical access to IT environment should always be protected by management from accidental or environmental damage, theft or inappropriate user access attempts. In so many cases, the inability to have the IT equipment in its own secured, environmentally protected room means management does very little else to protect the equipment beyond normal building security. Protection doesn’t mean creating your version of Fort Knox, restricting easy access to the network equipment is paramount to data security. If someone wants to set down a cup of coffee, make sure it’s not near the server; should someone want to disrupt normal business operations intentionally, then make them work for it by having the equipment in a locked server rack or cage. Hopefully, someone will see them during normal business operations or the police will have arrived to catch them in the act after hours.
9. Vendor Management or contract monitoring sounds easy enough, but for those businesses using another entity to perform a service for them (i.e. data center or application hosting, payroll processing, 401k or employee benefit plans) would mean reviewing a SAS70 report, Sys Trust report or PCI compliance certificates. Reviewing these reports whenever their issued is important to identify if the controls you or your external auditor rely upon on are in place and working appropriately. If there are repetitive issues identified on the SAS 70 reports, you may want to rethink you service provider relationship. A consistent issue may mean the service provider cannot control or adequately

protect your data and you may want to consider negotiating for better terms, request management provide more information on how they're safeguarding your data or changing service providers all together.

10. Backup Operations cover all the computer processing or controls used to maintain the physical equipment through daily backup operations or job scheduling. Most businesses perform some type of backups but whether it's daily, weekly, incremental, differential, or full is not nearly important as just performing them on a consistent basis. Having a backup process in place could mean the difference of having your business intact after a disaster, theft, misapplied update to the network or financial application, or a critical document being lost forever. What happens all too often is that management doesn't consistently monitor their backup operations or know if the data can actually be retrieved off the backup tape, disc or external hard drive. Performing an annual backup restore test at the database level will help to answer those questions in the event you need to do this process for real. If the system needs to be recaptured back to a certain point in time, doing this for the first time can be a one or two man fire drill. It also goes without saying but worth reminding business owners should remove sensitive backup data from the normal business location on a rotating basis to a neutral location for safe guarding in the event of a fire, natural disaster or theft.

We welcome the opportunity to meet with you to discuss how we can help you meet your business goals. If you have further questions or would like to request an IT Risk Assessment, please contact Sandra by e-mail at sandra.johnson@bakertilly.com or phone at 612 876 4857.