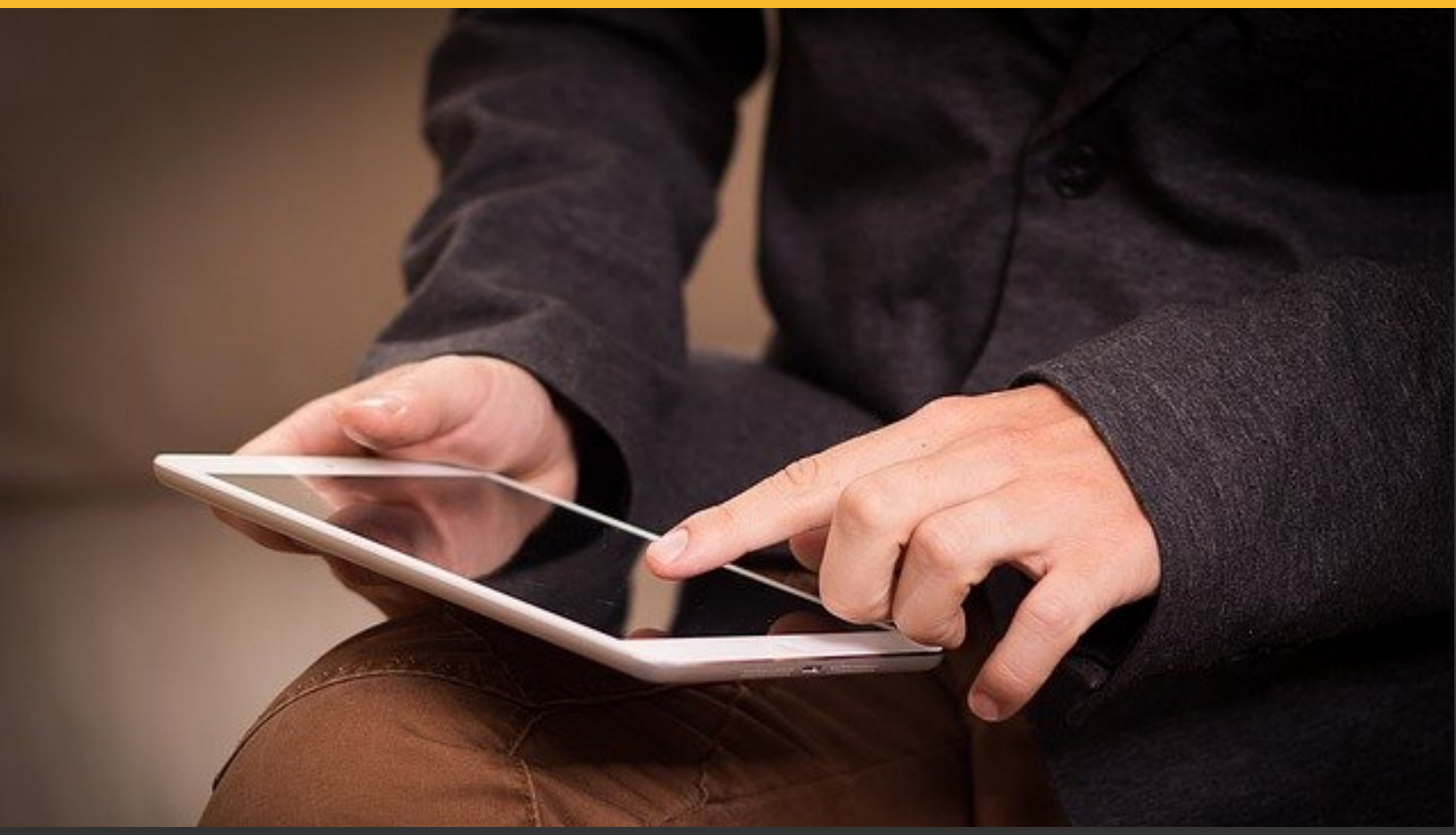
Knowing the Signs of a Failing IT Vendor



Kenji Martinez

Contents

Kenji Martinez

President's Introduction

Kenji Martinez, Founder and CEO of Oversight IT Consulting, is a Technology Solutions and Vendor Management Consultant from Los Angeles, Ca. His success in consulting small to midsize businesses and municipal entities is formulated from his unique approach to Information Technology Management. Kenji's tactical approach to managing staff and vendors has been successful by establishing unbiased consulting and evaluation services. His evaluations of IT vendors and proposed projects give oversight into financial and technological impacts of projects. Each client is provided with qualitative reports and communications guiding executives to confidently conclude and approve milestones, initiatives, and procedures to establish a highly available, robust and secure networks.

Overview

Vendor changes and management are challenging items for many companies. You hire them expecting performance, efficiency and a knowledgeable staff in fields you have little to no understanding of. So how do you understand signs of risks that may lead to catastrophic damages? Do you wait until you are disclosing data loss to a governing agency and your clients? So why should you wait for a major compromised network and become liable for data loss or loss continuity of operations to reassess your IT vendors?

There are many signs and important details that every company and manager of the IT vendor should be asking about. Here are the top 5 signs and questions to help you re-evaluate your vendor and decide if they need to be given a performance improvement plan or be changed immediately.

Top 5 Vendor Evaluation Key Points

1. Quarterly Reviews

Quarterly Reviews of your infrastructure, security and compliance.

For some vendors, this may not completely apply but it needs to be addressed. Clarify what services and items they are responsible for. It is common to have a perception that your IT vendor “does it all” but you need to keep in mind that every IT vendor specializes in specific items and will never cover all things. Some of the important questions to ask are ones such as:

What are the major concerns that we need to look at as first priorities regarding infrastructure, cybersecurity and meeting mandated compliances?

Your vendor will most likely point out things like, “we do not attest, certify or take liability for you achieving compliance”. Understanding your vendors positions on what is being handled will ensure you are protecting your company against any neglect against your preventative maintenance, security and compliance.

If your vendor is providing security- When was the last penetration, risk and/or vulnerability assessment for our network?

Many and most compliances will require a “pen” (penetration) test, risk assessment and/or a vulnerability assessment. Many are external scans to see what vulnerabilities exist internally and externally. You must understand that software and hardware is in a constant state of updates. There is no answer to achieving a 100% remediated and hardened environment but creating a gap analysis will help keep your cyber hygiene at its best. As a best of industry standard your provider should be recommending and you should be asking to perform, at a minimum, a pen test and vulnerability assessment. The tests are commonly inexpensive, and you may be shocked with the levels of exposure that can be easily remediated. This also a great way to point out where the vendor is lacking focus.

What items should we be budgeting for in the next quarter and the next year?

Your vendor has the keys to your kingdom and should be running what is called an RMM (Remote Monitoring Manager). The RMM is responsible for gathering network health statuses, serial numbers, firmware updates, OS (operating system) versions, data from the last user’s login and more. This information is easy plugged into subscriptions your vendor should have that automatically generates when the workstation was purchased, how long the warranty is and it the warranty has expired. This information can be generated and exported to excel within a matter of a couple minutes.

From the reports and collective ticket data, a vendor should be able to point out what hardware is end of life, failing and systems need to be repaired.

When was the last audit completed to check identity and assets were properly given and revoked in the last quarter?

Access, role change and Identity management are two large factor that can cause issues such as accidental deletion, successful insider threats and granting access to confidential information to employees or outsiders that do not have proper clearance to access the data. Reviews should be done at least quarterly to ensure terminated employees are removed from domain access, email services, cloud-based services and more. Your vendor should be using forms that list all services and devices that exist with your company. When employees are onboarded or roles change, the document should be filled out by the HR or management team and submitted to your IT vendor to implement the changes. When the notices are sent to IT to remove access, the IT should be responsible for going through a check sheet to show they successfully removed access from the known systems the employee had access to and validate they checked remaining systems to ensure access was fully removed.

When was the last time they restored your backups and tested the data integrity?

There are two types of backups- file and image level backups. Either way, the most important thing about backups is they are tested and restored. You are paying monthly to ensure your business is not taken by ransomwares or physical failure. If you are paying for image level backups, it's a little more expensive but it creates a virtual copy of your servers that makes restoring the backups much quicker. The applications and configurations restore all in one shot and can be restored in a data center or on premise depending on your business needs. Failing to test and restore the images can lead to issues like spending days rather than hours to restore servers and operations. To protect yourself from vendors billing you for the restoral at a file level, when you paid for the image level to be backed up, is to ask about when the last restoral and test was completed.

Task	Date	Notes	Complete
Create PO	Thursday July 16, 2020		✓
Sign PO	Friday July 17, 2020		✓
Send PO to Dell	Friday July 17, 2020		✓
Forecasted Hardware Rec'd at XX corporate building 555 North St. Somewhere, Ca. 55555	~~Friday July 31, 2020~~ Tuesday July 29, 2020	UPS Tracking number 1Z82749SE003	
Forecasted Hardware racked and mounted (technician, John, onsite)	Wednesday July 30, 2020		
Forecasted Servers formatted	Friday August 1, 2020	Dell support required. Confirmed Dell appointment 8.1.2020	
Forecasted Server configured	Friday August 21, 2020		
Forecasted Server Quality Check by second engineer	Monday August 24, 2020		
Forecasted Initiate 1st Backups	Friday August 28, 2020		
Forecasted Initiate backup restoral and testing	Monday September 7, 2020		

Example Template of Project Milestones and Progress

Are there any business impacting deadlines that need to be met in the next 12 months?

The worst factor that can happen with a vendor is they fail to be proactive and cause down time to your operations. It is known that network reboots after updates are necessary but there is a fine line between neglect and unforeseeable circumstances caused a lapse in network or system availability. The vendor should be aware of any notices you received from a partner, governing agency or application alerting there will be a mandatory shut off or lapse in services if a compliance deadline is not met or update is not completed. The quarterly meeting should be outlining the priority of projects and imposed impacts if they are not met. Large items based around loss of operation and compliance mandates should be resourced with a project manager to outline the weekly or bi-weekly milestone progress to completing the task. This level of transparency should show the level of involvement and productivity being resourced into your systems. These notices are as easy as an email template that detail the progress, project milestones and projected dates to keep pace and expectation with the engineering behind the implementation. This progress should be handled by a project or account manager who can oversee all working component- the technicians, supplies and third-party vendors.

2. No response or follow-up to project engineering or project proposals

If your vendor identifies a risk or opportunity to optimize your environment, they should be emailing and calling you continuously to make sure the project or issue is thoroughly explained, acknowledge and vetted. If you find that your vendor is constantly throwing emails into your inbox stating they found an issue with a drive that might fail or your firewall subscription was not renewed on time but do not call to discuss or show up on site to explain the business impacting reason it was sent you should highly consider this a “pass the buck” tactic. They notified you and left the liability in your inbox with 13,940 unread emails that you didn’t read and respond to for them to make the critical decision to remediate or repair something that ultimately impacted your operations, reputation or compliance.
Important questions you should ask yourself to evaluate their commitment to you:

What is a reasonable amount of effort to notify me about something that can potentially hurt my business?

Every IT vendor has SLAs and a tier of severity scale for technical issues. Does your vendor notify you the same from their top tier to their lowest? Ex. Email quarantined vs. email compromise. Are they both an email response if any?

Is there an incident response plan your vendor has in place to properly respond and receive approval for mission critical decisions?

This is critical to those who are regulated by compliances such as HIPAA, FINRA and CMMC. Each compliance mandates breaches of information are to be reported within a specific amount of time.

What are the lead times to receive engineering and quotes for projects?

Does your vendor have a quote or engineering responses back within five business days? Granted some projects are larger than others. When a project moves past the five-day mark is there communications that they are working on it or are they buying time with constant responses like “we are so close and almost done… just hold tight”? This could be a sign that your vendor is overstretched and low on resources to handle a project.

Delayed Implementations

3. Delayed implementations of your projects or irregularly long completion times.

It can be difficult for IT vendors to understand that they need assistance. Some vendors think they can learn and do everything themselves but there is a very important aspect many people forget to keep in mind about IT- Information Technology is always evolving, becoming more complex and requires more skill sets than one organization can hire. This is where the concept of ***Power in Partnerships*** is important to not only your business but your evaluation of your current or next IT vendor. Your ideal IT vendor should model themselves as Batman, who now has to strategically fill his toolbelt to assist with things outside the norm, outside the expertise and control of their specialized teams. There are many professional groups that handle and specialize in email migrations, SharePoint migrations, SIEM monitoring and so on. When picking a Managed Services Provider or Managed Security Services Provider, keep in mind their main role is to manage current infrastructure, assets, identities, basic to advanced security and not to migrate systems and services. They may have divisions or engineers that can handle these projects, but it is important to get quotes and even ask your current provider if they use a professional services team like Pax8, Rackspace and other certified teams for your project and investment. Some vendors are channel only and must be teamed with by your IT vendor, but this secures you against a couple issues like bill bloating, unexpected outages, compromises and missing implementation deadlines.

Tell tales that your vendor has overstretched their capabilities or resources-

- Implementation start dates for projects more than 30 days away
- Projects are not managed or are missing clear and distinct milestones
- Project engineering is lingering due to necessary calls to other vendors- "*We are still trying to get a hold of XYZ because we cannot move forward without their input.*"
- Bill Bloating

4. Bill Bloating and Disputes

Many teams are busy migrating the data and information is not properly recorded in the tickets that lead to machines being replaced yet the old machine was not removed from services and is still being billed. If you find discrepancies, you can ask for the endpoint list for each quarter to then identify what machines have been added and who the last users were. At this time, you can identify if your vendor is proactively managing your assets and identities that you are being billed for and if they are following compliances that require asset and identity management.

In an Oversight IT Consulting contract from 2020, a vendor was third party audited for their identity and asset audits. The vendor stated they audited every 30 days before monthly statements are sent for accuracy. Oversight IT consultants researched the original support contract extensively to find an

over billing of 25% each month (~$900/mo) for more than 1 year of services.

The contract was followed, client was credited the overages, and a new SOP, Standard Operating Procedure, was presented to the MSP in order to properly audit for services, users, and subscriptions.

The last item to consider about billing is how often do you have to revisit bills and dispute charges? If you are an attorney that charges $500 per hour and you spend 2 hours disputing your firms IT bill for $900, you can be spending up to $1,900 for IT services. You are losing your productivity, costs to cover an employee to audit and dispute the IT bill and even billable time to your clients when you missed the sales lead on line 2 when you were busy disputing the IT bill. Established IT vendors should have a transparent break down to show what services are in and out of scope in your monthly maintenance that is backed by a billing department. Any billable work completed by the vendor should be documented with what day, time, ticket number, person performing the remediation and notes detailing the issue and actions taken to accomplish remediation.

Red flag signs to audit for:

- You pay monthly for an onsite technician to perform work on a scheduled basis and you are being charged out of scope for a project or ticket during the scheduled time by the onsite technician.

- More than once a year you get “you are right, let me remove that right now”. Common issues with the billing are items are passively added in small detail and never audited. Great examples of this were the beginning of the smart phone era- how many times did you catch “navigation” or “music” apps on your bill. The trial was great until you realize they didn’t confirm with you to keep the services or remove it, leading you to now pay a full rated service for something you may not be using.

- You are finding decommissioned endpoints or terminated users are still being billed.

5. How Well Do You Trust Your IT Vendor?

“Breaking up” with your IT vendor can be mentally straining and intimidating. You should never have to feel that a vendor is holding you hostage or will ever retaliate against your organization. At the end of the day, you must remember who needs who, they **want** your business, and there are hundreds of qualified firms that are available in your area, let alone by remote access nationally. If you find yourself questioning the integrity or ethics of your vendor, it is time to consider a professionally managed team that is attested for strong compliances such as CMMC or NIST 800-171 (a stricter and well-defined compliance compared to FINRA, HIPAA and PCI). Compliances such as these require technical controls like using encryption (protection of sensitive data and credentials), separation of duties (they don’t have their techs using super admin credentials while doing work), audit logs (to be accountable for all work performed and tracking of any compromises) and least privileges (does not give access to users unless it is essential for them to accomplish their role) are in place accomplish protecting you from error and compromise. The controls are important to ensure that the new age of cyber compromise, who by the way target MSPs and MSSPs since they hold the keys to everyone’s infrastructures, and aides you in finding a vendor that will be liable for technical mismanagement and subject to audits and fines for not proactively securing clients data.

Red flags to validate your concerns:

• You feel “bad” or a “nuisance” to call in about small issues

- **NO** IT vendor has the right to make you feel like you cannot use the services that you pay for or that you are a burden to them

• Your IT “guy” is always upset, grumpy or talks in technical jargon and doesn’t try to help elaborate in a manner you can understand

- Your IT vendor needs to cooperate as a partner and act like an employee- professionally and diligently

• If you find yourself keeping all emails and tickets to keep your IT firm accountable when the bill comes
• You feel they will retaliate if you send notice of termination
• You feel they can see your activities and emails remotely and without authorization
• If you have ever had a dispute over the work performed and they did not show documentation

• If you feel they are never around, and you wonder what they are doing

- Most companies work behind the scenes but quiet isn't always good. Your environment is always evolving and changing, there should be contact to ask for directives on scheduling firmware and security updates or lifting security stands to meet the new mandated state, federal and international compliances.

• You inquired with your IT vendor about how you think you were compromised, and they didn't instantly respond or downplayed the odds of you being compromised

- Ransomware, viruses and phishing scams have become more complex. It is dangerous to assume that a compromise is just a misunderstanding. More commonly, viruses are found in order to make technicians think they have found the infection and compromise when a slumbering ransomware is rooting into your servers and domain controllers.

- On another note, more frequently IT compromises are found in the lower supply chains of major companies. With tighter budget, lower priority focus on cybersecurity, outsourced IT support, and commonly with the mentality of "why me, I have nothing worth compromising", lower supply chain suppliers are easy targets and often have data or access to data of a larger company.

Making a Change

Now that you have identified if your vendor is proactively providing the services as promised, if you have found yourself frustrated, validated or enlightened about a vendor that is mismanaging your business you need to know some key things to help minimize the impact of changing vendors.

- Request a conference with your IT vendor.

  -Identify any outstanding tickets, projects and issues.

  Document these items and create a list for them to respond in order to project manage the completion. The vendor should identify how long the items will take to resolve and have them email you a confirmation acknowledging the outstanding work to be finished with projected completion dates.

- Use the knowledge learned to evaluate vendors and take multiple proposals.

- Stop using “your friend’s son” or “Uncle Bob’s best friend’s son’s fiancé’s company” without qualifying them as a valid vendor. Technological knowledge is often misconstrued with people that have technology. You need to see the proof in the writing, look for certifications that match your environment.

  -Microsoft or iOS- are they certified Microsoft Partners?
  -Servers- are you physical or virtual servers and are they on premise or in a data center (cloud) Are they certified in VMware (managing virtual servers), Citrix, Azure, AWS?
  -Firewalls and access points- are they certified with your manufacturers (Cisco, Barracuda, Palo Alto, Watchguard, Datto and etc.)
  -Backups- do you have backups? Are they certified with the provider? (Datto, Acronis, Veeam and etc.)
  -Applications- do they have past performance supporting the applications? Don’t be afraid to ask them for references with existing or past clients that they support with the same applications.

- When you find a firm you like, plan at least a two week to one-month transition plan (yes you will be paying two companies at once). This ensures credentials are properly handed off, validated and accounted for. Even in a great handoff between companies it is important to understand that credentials can be anywhere from 10 to 100s of usernames, passwords and URLs required to access the administration user interfaces.

- Before the final day of your outgoing vendor's services, request an account manager to have direct contact with incase any technical knowledge or remaining credentials need to be gathered.

  -There are many nuances to an infrastructure each technical group provisions and configures things differently. If there is any failing hardware being inherited by the new vendor, you may need to understand how the previous vendor rebooted the systems when they were non-responsive

- Enjoy the new vendor and review their performance every quarter. Vendor Management is key to success and falls under the same theory of managing employees, it takes revisiting and work. Give them progress reports and never feel ashamed to give feedback if its good or bad. The good reinforces the positive actions and the bad are necessary to create Corrective Action Plans, CAPs or Performance Improvement Plans, PIPs.

- Work with your vendor to identify your next technology vendors, i.e. Cybersecurity, applications, telecommunications equipment, compliance assessment firms. Each vendor should work with you as a partnership assist as a council when you are in need to industry knowledge and recommendation.

- Going forward, ***ALWAYS GET MULTIPLE BIDS!***

Get in Touch!

If you find yourself overwhelmed and require a professional IT consultant to guide your organization to a qualified IT vendor or wish to get second opinions about IT initiatives, reach out to Oversight IT Consulting for an unbiased and vendor-agnostic approach.

Kenji Martinez
Founder and CEO
Kenji@OversightIT.com
www.OversightIT.com