Guide to Overseeing IT

When IT is not your day job

By Ryan Barton

Ryan Barton is the founder and CEO of Mainstay Technologies,
based in New Hampshire. You can reach him on LinkedIn
or at rbarton@mstech.com.

The problem: IT is complicated and getting more so each year. It impacts every area of the business. IT must be led well, so you have confidence that complexity is being leveraged *for* your organization, not against it. For business leaders who aren't directly technical… how does one ensure that is true?

When I started in this industry, clients would tell me "I'm not worried if email goes down, our clients will just fax us." Or "Do I really need a password on my computer? There's nothing in our systems anyone would care about."

How times change. And there is no sign of technology's growth slowing!

Business leaders must have a firm grasp on IT's risks and opportunities. However, because of the complex landscape, the acronyms, and the rapid change, business leaders ***often believe that clarity and confidence in IT requires technical knowledge***. Not being technical themselves, they end up settling for a general sense of concern, which makes them over-reliant on their technology staff and partners.

This is a bigger problem than they realize.

IT *is* my day job. My company wrestles with IT complexity so our clients can have justified trust in their IT and a technology experience they enjoy.

Last month, we were called by a NH firm after hackers took total control of their systems, threatening to release sensitive data unless an enormous ransom was paid. The IT people this company relied on were all nice and well-meaning. The only malfeasance was by the hackers. But the IT protections were suitable for 2015, not 2022. And the business leaders didn't know it. Their inability to ask good questions, to know the landscape, and to assess their IT appropriately meant the true risk stayed hidden. It was only after a catastrophe they realized their risk. Thankfully, we were able to recover all their data and secure them appropriately, but not until after the significant pain of downtime, cost, and reputation hit.

So how do you know if IT is being led well, if you're not technical? Not by becoming technical, but by understanding three core principles:

#1 Expect Clarity

Author Brené Brown has said, "Clear is kind. Unclear is unkind." Clarity is the responsibility of the technical team. If they can't provide you with predictions, a roadmap, and context to make good decisions, that is a failure of their leadership – not yours. If you have questions about the cloud, about cybersecurity risk, and about proactive measures that aren't answered with the options, metrics, and detail that gives you exactly what you need to make a decision, that's a problem.

I am not an attorney. But as a business leader, I frequently need legal advice. The role of the attorney is to wrestle with the complexity of the law, to give me good guidance. I expect options and clarity on the potential consequences of each option.

IT must do the same. If it doesn't, you accept a risk level similar to a business leader crashing through M&A without the benefit of an attorney. Maybe things go well. Maybe?

IT wasn't always this way. But with the cloud, complex cybersecurity layers, interconnected software, large databases, and your staff working from anywhere, your clarity over IT is imperative.

#2 Think of "Technology" in 4 Categories

"Technology" is a big word. If you ran a 1,000-person organization, you'd likely have a high-end technical business leader called a CIO who handles all this. Below that size, the leadership team must simply recognize 4 different business units (or areas) of technology that require slightly different intentionality:

1. *Software.* The *software* you use and the *business processes* that surround the software. Each industry has their own software – law firms especially – and the way you use the software, train staff, and integrate technology makes a significant difference in the organization. In less-than-200 person organizations, this is usually led by practice (or department) heads and relies heavily on industry software vendors.

2. *Data, Business Intelligence, and Reporting.* The data you have, the databases and folders that house it, and the insights you are gaining from it. BI (Business Intelligence) and Reporting lets you ask questions of your data and drives better decision making. This responsibility is often shared between some internal staff and a software vendor.
3. *IT & Cybersecurity.* Your IT department/partner – tasked with keeping systems stable, fast, and secure. This includes future planning, proactive measures, cybersecurity defenses, monitoring, and response to any issues. In less-than-500 person organizations, this is typically outsourced, as some scale is required.
4. *Information Security & Compliance.* This is about the compliance of your whole organization. Security not just of the technology, but of the firm. Legal compliance, and protection from data loss, both require a dedicated approach to policy, process, manager training, and risk identification. This is the realm of Risk Assessments, System Security Plans, and Information Security Program Managers. This is nearly always outsourced, until an organization is very, very large.

In a healthy organization, all 4 work smoothly together, serving the leadership team to leverage technology, support it well, and secure it.

#3 Ask Questions

Be curious about the details. For IT, ask at least these 8 questions:

1. *To your staff:* How is your experience with your technology? Is it reliable and fast?
2. *To your staff:* How is your experience when there is an issue? Is a resolution speedy and the experience agreeable?
3. *To your leadership team:* Are you held back by IT in any areas?
4. *To your leadership team:* Are we confident we are on the leading side of our industry, in terms of software, data, and risk?

5. *To your IT:* What kind of infrastructure are we moving to next, and when and why? (if the answer doesn't involve the cloud, ask a lot of questions about why *not* and ask to see comparisons with pros and cons)
6. *To your IT:* How many of our systems have 100% of their patches installed? (this is a great way to tell if the hard details of IT are being owned properly)
7. *To your IT:* Can you please provide me a copy of our Disaster Recovery Plan, asset inventory, and a graphical diagram of our IT systems, and explain each to me? (These are the bare minimum of what IT should be documenting, even in a 5-person organization)
8. *To your IT:* How much risk do we have in cybersecurity, and what are the next 3 most cost-effective things we can implement to lower the risk?
9. *To your IT:* Do we have Multi-Factor Authentication on all external access, including email, IT access, VPN (Virtual Private Network), and cloud software? (If the answer is no, be very worried. Multi-Factor Authentication is incredibly low cost, often free, and without it a breach is simply a matter of time)

How much should you worry about IT? It is a question worth asking. If the answers you receive from the questions above give you clarity and confidence, then sleep well.

If not, then the growing complexity of technology has overwhelmed your current IT structures. And this risk is not one to ignore.

Every organization must have trustworthy IT, led by a technical team they enjoy. And every business leader overseeing IT must have clarity of direction and confidence in results.

Contact us for more information about IT & Information Security services.

mstech.com/contact • info@mstech.com • (603) 524-4774