David Kay

DB Kay & Associates

Practical Trust
How to Make Organizations Innovative, Efficient, and Engaging

What if Your Company Trusted You?

If your company trusted you, you'd have significant freedom over how you did your job, but a very clear view of what you're supposed to be delivering, and why it's important. Enterprise applications would require a fraction of the work they do today. In a trusting environment, you'd enjoy your workday more.

I started thinking about trust because my firm focuses on a way to share knowledge in which workers create and update structured bits of content as they do their job. Sounds reasonable, right? You might be surprised at how controversial it can be! The employees resolve customer issues, but leadership doesn't trust them to write that same answer in a knowledge base. So, I experienced how trust is an essential element for our clients, and as I looked across enterprises, I realized how universally important trust is.

Trust can be built with intention. This paper will make the case for doing so, and then provide some guidance on how to do it.

Mistrust is the Default

When I first moved to Silicon Valley, there was a Mecca to visit: Fry's Electronics. Their handful of stores featured inspired design themes like computer chips or ancient Egypt. If you were a nerd like me, they had everything you could possibly want, from soldering irons to integrated circuits to every component you would need to build any kind of computer to—inevitably—snack food. It was a treat to shop there.

But after not very long, the appeal wore off. As magnificent as the stores were, there was always something unwelcoming and off-putting inside. After a while, I figured out what it was: extreme, maybe pathological, mistrust.

To release any product of value, or to sign off on anything, a cashier would have to go back to a second row of desks to get approval from a superior. Often the superior would need to talk to their superior. It wasted my time, and it seemed demeaning to the people doing the work. "Loss prevention specialists" checked your receipt and your merchandise as you left. Oh, and good luck if you ever wanted to return anything. It was all kind of ugly. I stopped going.

What if, instead, the company trusted the people doing the work—if cashiers at Fry's would have been able to complete most transactions themselves? That's how my local Rural Supply hardware store works. Workers take the initiative help you find things, choose products, and plan your job. The registers are staffed with what appear to be high-school kids, but they don't seem to need any help or approvals checking me out. If I can buy what I need from Rural Supply, I'm going to buy it there.

The question at the top of this paper is the foundation of Michalski's "Design from Trust" initiative. It's a disarming question, because asking it in regards to almost any institution or process illustrates how our culture instinctively chooses mistrust as the default setting. Michalski is focused on rethinking really big areas of the world: education, civic behavior, and government. As a management consultant, my view is more focused: how can trust improve the value of what we do at work, at the same time making the workplace better for everyone involved?

The State of Trust at Work

Unfortunately, the same mistrust-as-default infuses most enterprises, even with valuable, highly-compensated knowledge workers. How do we know this? I'll give you three snapshots: rules, software, and monitoring.

Very Specific Rules

In customer service or support, managers will evaluate a certain percentage of customer interactions to make sure that all the rules were followed—rules about how the agent greeted the customer, how they managed the call, their professionalism, and how they closed the call. There are typically something like 20 rules like this, and if you don't follow one of them, you fail. Agents have to tell customers to reboot their cable modem even if the customer pointed out that there's a neighbor-hood-wide outage. Agents have to ask "Is there anything else I can help you with?" when they know good and well that the customer is running late and just wants to get off the call. In other words, these rules can make people who were hired for their people skills do things that defy common sense and ignore their intuition.

I've worked with organizations where front-line staff have to hand off a call to a higher-level person after a half hour, even if they're a minute or two away from resolving the issue. That's the rule.

In a TED talk, Barry Schwartz tells the story of an actual absent-minded professor who mistakenly gave his underage kid a hard lemonade at a ball game, not understanding the implication of "hard." A security guard saw this and, although the nature of the mistake was obvious, the guard had to follow the rules, so he initiated a process that resulted in the child being taken away from his family—fortunately, temporarily. The security guard knew what was going to happen, and that it was inappropriate in that case, but…the rules are the rules! As Schwartz concludes, "Rules make you stupid."

I want knowledge workers to use their judgment and intelligence to solve difficult problems, to innovate, and to improve how they do their job every day. The last thing I want them to worry about is being compliant with picayune rules.

Enterprise Software

Many knowledge workers are aided by software that helps automate the routine parts of their jobs. At their best, these tools eliminate drudgery while improving consistency. A part of their power is the extent to which they're configurable. Every company and department does things a little bit differently, and the tools need to support these variations.

One of the most implemented configuration features is permissions—making sure that someone you don't want to do something, can't. Business owners want increasingly fine-grained control of these permissions, because they want to make sure people can do all the things they actually need to do, and not a single click beyond.

Increased granularity of permissions leads to increased complexity of the already oversized software implementation process, both for the vendor and the company using the product. In the enterprise applications I'm most familiar with, 90%+ of the unexplained errors that bedevil users and administrators are caused by mis-set permissions. This isn't because administrators don't know what they're doing; it's because it's nearly impossible to get something this complex right for everyone or when rolling out new capabilities.

Constant Monitoring

George Orwell got it mostly right about ubiquitous surveillance. What he didn't envision was that not only can the government watch almost everything you do, but your employers can, too. For many knowledge workers, starting their workdays is entering the Panopticon where they can be watched at any time without knowing it.

There is software that takes a screen shot of each worker's desktop randomly every five or ten minutes, so supervisors can confirm that they're always working. The same software can log each keystroke for review. I talked with one senior leader who had deployed this software; he flatly said, "There is no expectation of privacy at work."

Artificial intelligence and machine learning give enterprises far more sophisticated tools for tracking and grading workers. In customer service and support, vendors are selling tools that perform sentiment analysis to look for agents who appear to annoy too many customers. Unlike human QA, this software can judge literally every minute a knowledge worker is at work. Also unlike manual QA, there is no considering the context, as there would be with a human. If the algorithm calls too many strikes, you're out. Or your pay is docked, or you won't be promoted.

If you trust people, you don't invest the resources to track them all day. Since our companies do invest in monitoring us, we know they don't trust us.

Most People Come to Work Wanting to Do a Good Job

My belief is that most knowledge workers you hire want to do a good job—to help their company, their coworkers, and their customers. After all, there is tremendous satisfaction in a job well done, especially if the company recognizes you for it, the work is interesting, and others rely on it. To me, this forms a valuable basis for trusting people unless they show us they're not worthy of it.

What Happens When We Trust?

When we extend trust, the workplace is a better environment.

Workers Tap into Their Wisdom and Creativity

Simon Sinek's Golden Circle tells us that workers want to know not only *what* it is they're supposed to do, but *why* it's important that it gets done. The *why* should be something bigger than the company: "creating shareholder value" is not very exciting. On the other hand, working for a healthcare company that aims to "rid the world of fear of cancer" sounds pretty inspiring, especially if workers understand how they're contributing to that vision. Workers who believe in what they're doing produce better work and get more satisfaction from it.

When you focus less on compliance and more on the what and why, workers apply their own common sense and good judgement to do the right thing. This is especially true for customer-facing roles. A luxury hotel brand gave all its employees, including bell staff and housekeepers, a budget to do something nice for guests who ran into a problem or frustration at the hotel. How they spent it was up to them, based on their read of the guests: a bottle of wine, a bouquet, or a stuffed animal were all good. The hotel recognized that no one was in a better position to make that judgement than the employee engaged with the guest.

Opting to trust is how compliance turns into alignment and how managers turn into leaders.

Needless Inefficiencies Disappear

When knowledge workers feel trusted, and when they're not being micromanaged, their performance can blossom. When they have a say in how they do their jobs, they can tap into their own experiences and their ingenuity to identify opportunities to make things better. After all, they're the first beneficiary of process improvements. Empowering them with their own performance data makes sure that everyone understands the positive effects of their actions.

Rolling out new capabilities in enterprise software becomes simpler and faster, and administering it becomes easier. If we trust people to use software the right way without byzantine permission sets, complexity melts away. Besides, generally the challenge with enterprise software is getting people to do all the things they're supposed to do, not keeping them from doing things they're not supposed to.

Everyone Enjoys Work More

Most knowledge workers strive to meet high expectations. By eliminating picky rules, simplifying our software, easing up on the monitoring, and telling workers the what and the why, we create an environment for high performance. We help bind people together in collaborative teams. And as I hope you know through personal experience, it feels great to be part of a high-performing team.

Soldiers, sailors, airmen*****, and Marines who have been in combat, in constant danger and facing extreme challenges share a common experience. The only way to approach their mission is as a tight team. They trust their superiors, but more importantly, they trust each other with their lives. Bonds they form in the crucible of combat are as close as any a human will know. I hope none of you are taking incoming at work, at least not in a literal sense. But with the power of trust, our relationships will be stronger, and relationships are something that humans are hardwired to feel good about.

Trust Smart

We used to give people more leeway, in part because much of the technology for mistrust didn't exist. We gave people telephones, and expected them not to make prank calls at work. We gave people email, and presumed they wouldn't write to customers to tell them they were idiots. Knowledge workers rarely clocked in and out: if there was time accounting to be done, we trusted them to do it themselves. It generally worked out pretty well.

Of course, sometimes it didn't. Trust is conditional, and if you show me you're not worthy of it, I will stop extending it, or extend it with significant caveats. This may have serious career consequences: who wants to work with someone who violates their trust?

We want to create a trusting environment, but we also want to keep our businesses, our employees, and our customers safe and secure. We want to use good judgement and not extend trust where risks are just too high. For example, if employees are surrounded by cash, as in a bank or casino, they should expect to be monitored closely. Or if employees are doing dangerous work like repairing electrical lines, we want them to follow safety procedures to a T. But knowledge workers tend not to be in those situations. Don't overestimate the risk of trusting at work—the risk you incur in most workplace contexts is easily outweighed by the benefits of trust.

I'm also not recommending that managers stop paying attention to the work their employees are doing. Managers should be looking for coachable moments, and should address real performance concerns directly. Besides, everyone likes to be paid attention to! This kind of normal human interaction is a far cry from the manifestations of mistrust we discussed above.

---

*Despite some controversy, the US Air Force has decided against using a gender-neutral word, so I'm using airmen here. See https://www.stripes.com/news/airmen-gender-based-job-titles-not-high-on-radar-1.416831

Practical Steps to Foster Trust at Work

When If you want to see the benefits of trust, you can start your culture change today. Here are three suggestions for doing that.

Be Worthy of Trust

Trust is a virtuous cycle: the more you extend it, the more others trust you, and the more you are trusted, the easier it is to trust those around you.

You can't control other people, but you're in charge of everything you do. So, behaving in a manner to build trust is essential. Be as transparent as you can be, within legal and regulatory constraints. Some facts are wise not to disclose, but others may just feel uncomfortable. Breathe through the discomfort.

Give credit to others. If you're a leader or simply part of the team, you look better the better the people around you look. You don't need to say anything about your contribution, in most situations—"the thing speaks for itself."

If you're a leader, and you say one thing when your team is in the room and another when they're not, you create a toxic environment for trust. Sure, there are things you can't or shouldn't share with your team, but what you can say should be directionally the same.

Do what you say you're going to do. If you can't, address the issue directly—explain why and what your Plan B is.

Work Incrementally

Culture changes don't happen on a schedule. You can't declare that you'll have a trusting workplace by 10:00 Pacific next Friday.

As with all culture changes, trust requires patience and a long series of small changes. Maybe you can stop looking at some measures for a while to see if people continue to do the right things. Maybe you can ease off of some monitoring. Or perhaps you might just let people do something themselves that previously required your approval.

One thing I've seen recently is the adoption of "do the right thing" vacation and expense policies, as pioneered by Netflix. Exempt employees don't have a fixed number of vacation days; rather, they take time off when it makes sense for them and their coworkers. Employees are counseled to make travel and other expense decisions in the company's best interest, without a long list of rules and policies. While some worry about employees jetting off on a month-long world tour or racking up exorbitant expenses, the reality is quite different. Most employees need to be encouraged to take more vacation!

Communicate the Why

With culture change, as with so much else at work, if employees know why it's happening, they're likely to engage far more productively. And this is all good news for employees: more autonomy, more empowerment, and more privacy.

Leaders need to paint a vision of a future state. It won't be a utopia: disappointments and imprudent actions will happen. But it will be so much better than today's workplace!

Some people just focus on the risk. Fair enough. The right way to frame this is as a balancing of risks. If we trust more, there's a risk our employees will cause harm, accidentally or purposefully. That risk is real. But what are the risks of not trusting? I hope this paper helps you communicate the downsides of mistrust. Then, you have open ground to make your case for the benefits.

We are here to help you when you start this journey.

DB Kay provides training and services for:

Knowledge Management with KCS®
Change Management and Culture Development
Customer Experience Journey Mapping
Taxonomy and Metadata
Self-Service
for market-leading service and support organizations

DB Kay customers include
IBM, Farmers Insurance, Extreme Networks,
NetApp, Palo Alto Networks, and GE

David Kay, principal of DB Kay & Associates, has been a leader in applying
technology to knowledge-intensive business processes like customer service since 1984.
He is a frequent industry speaker and has been recognized as an Innovator by the
Consortium for Service Innovation.

David Kay holds five patents covering the use of next-generation technology in customer service
and support. He is co-author of Collective Wisdom: Transforming Support with Knowledge,
available on Amazon.com, and author of Customer Service with AI and Machine Learning
on LinkedIn Learning.

KCS is a registered trademark of the Consortium for Service Innovation