tmb Group technology means business

Technology And Trust

How a measured, realistic and multi-layered approach to IT is the key to success and security

Trust plays an integral role in all our lives. We trust our family and friends to act in our best interests. We trust the use-by dates on food to stop us eating spoiled goods. And we trust the authorities and the government to carry out their duties.

In the business world, trust is just as vital. Whether it's our customers, our suppliers or our colleagues, our relationships are often shaped by the faith we have in the people and the organisations we deal with.

Increasingly, our personal and work lives are also being influenced heavily by technology. As technology grows ever more ubiquitous and more advanced, we're all handing over increasing amounts of control to it and placing our all-important trust in its supposed infallibility.

In this paper, we'll explore how trust in technology can go too far, leading to over-trust, a phenomenon that can damage organisational and personal relations and reputations. By examining this subject, we'll show how technology is essential to modern businesses, but that a multi-layered, well-planned and realistic approach is necessary to make the most of it.

How We Trust In Tech

The Oxford Dictionary defines trust as a "Firm belief in the reliability, truth or ability of someone or something."

It's easy to see how this applies to the way we use technology. When we log into our computers, we assume that everything will be how we left it, that our files will be saved in the same locations and that our favourite applications will work as expected. When software companies release updates, users normally install them without even testing them first. At airports and train stations, we gaze up at departure boards and treat their accuracy as a given. Every time you look at a digital clock, set your oven to a particular temperature, send a text message, set an alarm or buy a lottery ticket, you're placing your trust in technology.

> **"Because trust is so bound up in human emotion, we tend to react badly when that bond is broken."**

That trust isn't unjustified. Machines and computers are designed to do things accurately, over and over again, with far more precision, speed and consistency than humans could ever muster. It's these qualities of technology that have taken mankind to the moon, given us instant worldwide communication and fostered efficient global trade.

So important to us is technology, the annual Edelman Trust Barometer[1] has for several years found technology to be the most trusted of all industry sectors.

But, of course, technology can and does go wrong – and that's when the problems start.

The Danger Of Over-trust

Tellingly, one of the Oxford Dictionary's secondary definitions of trust is "Acceptance of the truth of a statement without evidence of investigation." Others, being less charitable, might describe that as blind faith.

In her paper 'When, How, and Why Do We Trust Technology Too Much?'[2], Patricia L Hardre explores the ways in which people put this kind of trust into computers, gadgets, machines and the information they produce – by default and without question. "Today," she says, "digital technologies, both tools and systems, function as replacements for trusted human roles." Furthermore, she states, "As a society today, we vest digital technology tools and systems with extensive trust and almost godlike power to control our daily lives and information needs."

It's this 'over-trust' that leads to what Hardre calls 'diminished vigilance' – essentially a fancy way of saying people let their guard down. Psychologically speaking, it's been shown that when people think someone is watching or monitoring a situation, they subconsciously become less vigilant of it themselves. And because humans have a tendency to anthropomorphise technology, imbuing it with human strengths and weaknesses, we're generally happy to hand responsibility over to it.

The consequences of such actions can be wide reaching, even fatal. If an airline pilot, for example, over-trusts his cockpit instruments, he may be lulled into a false sense of security, missing other potential warning signs when something goes wrong. In a real-life case, a pedestrian was killed by an autonomous car owned by taxi firm Uber[3], because the human operator was watching TV on her phone instead of monitoring the vehicle.

More commonly, over-trust in technology has less tragic results. People lose their entire address book, for instance, because it was stored on their mobile phone, which they dropped in a puddle. Or they blindly follow their satnav until it leads them into a river[4].

In a business setting, total faith in technology can and has led to major problems, one prominent example being the farce that followed TSB's migration of customer data to a new computing system. Having used the technology infrastructure of its former partner, Lloyds Banking Group, for some time, TSB understandably made the decision to move over to its own system. Millions of account details had to be migrated, but as we all now know, it didn't go according to plan. Initially celebrated as a success, with TSB employees posting photos on LinkedIn, showing them quaffing champagne and generally slapping themselves on the back, the project was an unmitigated failure. Many customers were unable to access their accounts, some could see other people's account details, and more than a few fell victim to fraud as a result. Weeks later, matters had barely improved.

While there was probably no singular cause for the TSB meltdown, a lack of adequate testing no doubt played a part. So too, it seems, did the over-trust of engineers and executives. Having successfully used the same software before, they assumed it would work again, even though the project in this case was on a much larger scale.

It's also clear that too much faith was placed in one technology – a common sign of over-trust. Businesses should always think about having some redundancy in their systems, in case the worst happens. For this very reason, experts recommend organisations implement a 3-2-1 backup strategy as a minimum[5], keeping at least three copies of important files and data, on at least two types of storage media, with at least one backup kept off-site. Relying on only one backup is a recipe for disaster.

> **"Every time you look at a digital clock, set your oven to a particular temperature, send a text message, set an alarm or buy a lottery ticket, you're placing your trust in technology."**

The Long-term Damage Of Over-trust

Over-trust in technology hurts businesses in a few key ways. As we've explained, it can result in a kind of complacency, where businesses leave themselves vulnerable. They assume their firewall will keep out 100% of attacks, that their on-site backup system will never fail, and that deploying new solutions will always improve workplace efficiency.

It can also give rise to a situation where belief in the technology supersedes faith in people. A user may complain that something isn't working on their computer, for example, but because they trust the system, the IT department may assume the problem is the user's fault, so they don't bother investigating.

This attitude can quickly see a small problem escalating into something much larger, although entirely preventable. And, as TSB discovered, beyond the immediate damage it causes, there's a much greater issue at stake – that of reputation.

Because trust is so bound up with human emotion, we tend to react badly when that bond is broken. When what is or is perceived as promised doesn't turn out the way we want, that trust can be shattered beyond repair. Businesses should also be aware, as Hardre puts it, that "clients, customers, and citizens attribute characteristics of the systems to the owner/sponsoring organization or entity". What that means is if your business suffers some kind of technological failure and it has an impact on your customers, they will ultimately place the blame at your door. Losing customer data or messing up orders because you've been hacked or a server has broken down is an ideal way to lose their trust and damage your profits.

Furthermore, in the same scenario, the company who falls victim to a data breach could lose trust in its cyber security solutions, causing it to ditch or change them unnecessarily and without addressing the actual cause of the breach.

What Are The Solutions?

Immediately, we should dispense with the idea that technology can be abandoned. Yes, it can be the cause of problems when it goes wrong, and yes, it can make people complacent. But it's also necessary, and the very fact it's so engrained in our lives is what makes it so painful when it's not working properly.

Without technology, businesses would struggle to communicate with suppliers, staff and customers. Record-keeping would become bloated and inefficient. Logistics would slow to a crawl.

Technology also offers competitive advantages, enabling smaller firms to punch above their weight and get ahead of the pack. Take it out of the equation and you're likely to get left behind.

To tackle the problems that stem from over-trust, you need to consider the well-known trio of people, processes and technology. The first challenge is changing the thinking of all stakeholders, getting them to realise that technology, while invaluable, is never perfect. It will always have limitations, potential flaws, incompatibilities and so on. In recognising this fact, people should see that personal responsibility and awareness should not be diminished by the technology that businesses employ. A practical example of this would be teaching staff to recognise phishing emails, rather than relying on automated spam filtering to catch everything.

This kind of awareness needs to be backed up by policies and procedures, which should make clear how your people and your organisation use and implement technologies. Well-documented and stringent testing, for example, should precede any major deployment of new systems.

Facts And figures

Although technology is the most trusted sector of all at 75%, that's among the general population. Among the informed public, Edelman points out that trust has slipped significantly, dropping in 16 of the 28 markets included in the survey. For example:

- US -19
- Hong Kong -14
- Germany -9
- France -18

While overall trust in technology is still high, that doesn't stretch to social media or search engines. In the UK, Edelman found that trust in social media dropped from 26% to 24% between 2017 and 2018, while search engines went from 54% to 47%. Of the Britons surveyed, 62% said they were worried that social media companies would sell their personal data without them knowing.

Finally, although it might seem like the cause of the problem, you can often combat over-trust in technology with more technology. One of the biggest mistakes a business can make is putting all its technological eggs in one basket. Instead, firms should be looking towards multi-layered solutions. As well as multiple backups, they should employ several types of cyber security, including a firewall, email filtering and anti-virus software. Where a multi-layered approach is not possible or appropriate, organisations should take greater care when rolling out new technologies, making sure there's adequate time and resources for testing. They should also keep one eye on the future, so new, market-disrupting technologies don't take them by surprise.

But most importantly they should understand that technology works best when it complements the efforts and decisions of people – not when it replaces them completely.

1) https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf
2) http://scitechconnect.elsevier.com/wp-content/uploads/2016/07/When-How-and-Why-Do-We-Trust.pdf
3) https://www.bbc.co.uk/news/technology-44574290
4) https://www.techradar.com/news/car-tech/satnav/the-uk-s-top-satnav-disasters-208089
5) http://www.tmb.co.uk/3-2-1-rule/