MIT MANAGEMENT SLOAN SCHOOL
IDEAS MADE TO MATTER

SUPPLY CHAIN 2020 SPECIAL REPORT

The new decade promises to be one of challenge and opportunity in supply chains. This four-article package describes all you should be tracking — and why.

CONTENTS

ILLUSTRATION: HUAN TRAN

ILLUSTRATION: ROB DOBI

These are the cyberthreats lurking in your supply chain

by **Tom Relihan**

Why It Matters

Effective cybersecurity involves more than just erecting a firewall. You have to clean up your supply chain, too.

YOU'VE GOT FIREWALLS IN PLACE. You have a team dedicated to keeping a careful watch over your networks, 24/7. Everything is under two-factor authentication. Your cyber defenses must be bulletproof.

Then your screen goes dark, and it doesn't light back up. Soon, your company is offline entirely, and you're losing money — fast. You didn't account for the contractor that you hired to upgrade your point-of-sale network last month, which required accessing your systems — or what the state of their own cybersecurity looked like.

Turns out, it's not good.

The vast majority of firms approach cybersecurity from a perimeter-defense mindset, focusing on keeping out hackers and other bad actors who shouldn't be able to access their systems, according to Stuart Madnick, a professor of information technologies at MIT Sloan. But organizations often fail to consider attack vectors originating, intentionally or unintentionally, with outside individuals, contractors, firms, or groups that are authorized to access those systems — so-called third-party or supply chain cyberattacks.

"The thing they aren't thinking about are people who somehow, one way or another, can slide right in," Madnick said. "Because once you've slid in, then all those perimeter defenses are next to useless."

Madnick, a founding director of Cybersecurity at MIT Sloan, said these types of attacks typically come in one of five forms: through physical parts or components bought from suppliers; through use of network service providers; from external software providers or partners; from physical service providers and outside contractors; and through mergers and acquisitions.

Here's how to defend against them.

Software service providers and outside contractors

For shipping giant A.P. Møller-Maersk, the installation of a single piece of accounting software in an office in Ukraine saw global operations grind to a halt and thousands of company computers rendered completely useless. That's because the smaller company that made the software, Linkos Group, had been compromised by a powerful piece of ransomware called NotPetya, which hijacked its update servers and used it as a beachhead to squirm into their client's networks. The results were devastating for firms across the globe, whose shipments were delayed.

The exploitation of smaller, typically less-secure companies who have access to or credentials for the networks of larger corporations for the purpose of either providing software services or contracted work is becoming increasingly common. Supply chain attacks rose by 150 percent between 2016 and 2017, according to cybersecurity company Symantec.

At Maersk, "It started off with a supply chain, which was the supplier of their accounting software, and that got it through the firewall," Madnick said. "More and more software services are providing automatic updates, so it's not an uncommon phenomenon."

In recent years, such methods have been attributed to major breaches at companies like Target, where hackers gained access through a contractor that performed ventilation work for the retail chain and made off with reams of customers' personal data. The U.S. electric grid has been targeted through similar tactics.

"A lot of these companies are vulnerable," Madnick said. "[Contractors] will come to your plant, and they may have their own laptops that they plug in to do diagnostic work, and you don't know what else they're bringing in when they plug into your network."

Any firm that plans to partner with a contractor or service provider would be well-served by conducting a security audit of that partner prior to entering into a contract or allowing any work to happen, Madnick said. Organizations could create a framework for evaluating and scoring a potential partner's security operations, or conduct "stress tests" on their networks. "You could then say, 'We will only partner with software providers who are level eight or higher,'" he said.

For the smallest of partners, like independent contractors who might not even have an IT or cybersecurity department, Madnick recommends they work with a consultancy to bring their defenses up to par prior to the partnership.

150%

Supply chain cyberattacks rose by 150 percent between 2016 and 2017.

"This can be a tough one, because you're talking about small organizations using unsophisticated systems and who don't have a lot of resources, and of course, the country is made up mostly of that," Madnick said. "You say, 'What's the big deal, why would Russia or North Korea want to hack into a company with four employees?' Well, that guy with the four employees is the access point to the U.S. power grid or Bank of America."

Mergers and acquisitions

Another potential point of complication for a company's cybersecurity landscape presents itself when a firm acquires a smaller firm or startup, or when two firms merge.

"A company maybe feels relatively good about security, but they've just acquired a company, typically a smallish one, and they want to, of course, get economies of scale and synergies. The question is, how good is the security in that company?" Madnick said.

The solution is similar: Do your homework before the merger or acquisition, don't wait until it's too late.

Physical components

Madnick said a third potential supply chain cyberthreat could be baked into the supplies themselves, either in the form of hidden "backdoors" embedded in software to allow secret, remote access, or through equipment outfitted with malicious hardware designed to steal information or hijack the system it's part of.

As far back as 2012, concerns about this sort of attack led the heads of the U.S.'s major intelligence agencies and House Intelligence Committee to advise Americans not to use products designed or sold by two Chinese telecommunications equipment makers, ZTE and Huawei, labeling such products as national security threats. In August of 2018, the Trump administration outright banned use of the companies' products by the U.S. government or any government contractors.

Global supply chains are also extremely complex, Madnick said, and it's hard to tell whether a particular piece of equipment has either been compromised by the manufacturer itself, or by other actors intercepting and tampering with it along the chain.

The best way to prevent such attacks is to keep close tabs on your supply chain, with the goal of being able to determine the provenance of each component, so that you'd be able to identify any points of contact that could pose a risk. "There are a lot of reasons you might want to do that, and there are lots of reasons why it's not easy to do," Madnick said.

Network services

Do you know the route your digital traffic takes from one point to the next over the internet? It's hard to be entirely sure, Madnick explained: Information sent across the internet from a computer in Cambridge, Massachusetts, to another in Washington, D.C., tries to find the fastest path there, not necessarily the shortest. That means your data could be routed through a hub in New York City, or it could pass through one in Beijing, if it reports faster speeds — where malicious actors could get their hands on it. This has actually happened, though allegedly only by accident, Madnick said.

Madnick says one way to defend against threats of data being intercepted and read during transmission over networks is to use encryption technologies like virtual private networks. Special browsers like Tor, designed to hide the location and other information about its user, can make it harder to tell when a lot of internet traffic is passing between two points, which could in itself be revealing, Madnick said.

Future threats

Looking forward, Madnick said a likely sector for future cyberattacks is the emerging "internet of things" — devices that connect to the internet for increased functionality, like home security cameras and lighting systems, and can be accessed remotely via smartphone or industrial equipment.

Any device that can be connected to the internet can pose a cybersecurity risk, and "the number of internet-connected devices is exploding," Madnick said. "The worst is yet to come."

Even more troubling, he said, companies tend to prioritize time-to-market for these products rather than than moving more slowing to ensure they're up to security standards. "IoT gives the hacker many more access points, and they're typically weaker access points, at least initially."

But, by incorporating cybersecurity into the design from the beginning, you can end up with more secure and higher quality products, Madnick said. 🏛

> *"Why would Russia want to hack a company with four employees? Well, that guy with the four employees is the access point to the U.S. power grid."*
>
> **Stuart Madnick** | MIT Sloan

ILLUSTRATION: ROB DOBI

4 ways to handle supply chain blind spots

by **Tom Relihan**

Why It Matters

Ethical landmines hidden deep in global supply chains can do serious damage to your firm. Here's how to avoid them.

DO YOU KNOW WHERE THE COBALT that helps power your smartphone or car came from, or who dug it from the ground? If it's an Apple device or a Volkswagen car powered by a Samsung battery, there's a good chance some of it was mined by Congolese workers under unsafe conditions — despite promises by both companies to clean up their supply chains.

But the complexity of those global supply chains, which cross oceans, borders, and cultures as they transform raw materials into finished products, makes doing so easier said than done.

Problems with ethical sourcing in supply chains have affected the textile, seafood, palm oil, and jewelry industries, among others, and could have national security implications. Nike faced pressure in the early 1990s over garments produced in sweatshops, and by the end of the decade, the company was forced to make widespread changes amid protests. Diamond mining giant De Beers, facing similar pressure over purchasing "blood diamonds" that fueled brutal wars in Africa, pivoted its business model to emphasize that its supply chain was free of the stones.

Greg Distelhorst, a professor of global economics and management who studies labor standards in the apparel industry, said building responsible sourcing practices in supply chains is an enormous task that takes a mix of technological innovation and relationship-building.

"The idea of a responsible supply chain is really simple: 'My dollar should not go to anyone who's profiteering off of slavery or worker exploitation or destroying the environment.' But the reality is so much more complex," said Distelhorst, formerly with MIT Sloan, now at the University of Toronto. "[Supply chains] have multiple layers, and at some stages in the supply chain inputs from one source and another source are mixed together in ways that are very challenging to provenance."

Here are a few approaches to keeping your supply chain clean and clear.

> “*The idea of a responsible supply chain is really simple ... But the reality is so much more complex.*”
>
> **Greg Distelhorst** | University of Toronto

Employ new technology for tracking materials

The biggest challenge to ensuring your company is responsibly sourcing its raw materials and inputs is getting an accurate picture of where they originate. In the Congo, the cobalt sold to battery maker Samsung, which supplies both Apple and Volkswagen, is sourced from both mechanized mines and ones worked by miners. The minerals are then mixed before being sold.

"Global supply chains often consist of three or more of these layers," said Joann de Zegher, an assistant professor of operations management at MIT Sloan who studies ways to develop innovative approaches to traceability in the first mile of commodity supply chains. "This makes the problem exponentially more difficult, as different tiers of the supply chain are further removed from each other and their commercial ties become more and more diluted."

Distelhorst said technology has begun to help in this area. Companies like New York-based Applied DNA Sciences have begun using molecular ink to tag products with plant DNA, while others use bar-code based technology to track products.

The tags are analyzed upon receipt to ensure a package received is the same one that left a factory across the globe. Organizations such as Starbucks and the U.S. Department of Defense have been counted among the clients of such companies.

"They're improving technologies around determining whether a shipment actually was built in a certain factory, and that's very promising," he said.

Other examples of technologies used to keep tabs on unethical sourcing include hotlines for workers and satellites to monitor both deforestation and the activity of fishing boats. The latter was used to uncover the slavery practices rampant in the Thai fishing industry — the world's largest supplier of seafood — when reporters from the Associated Press used satellite global positioning technology to track boats and shipments.

Eliminate incentives for unauthorized subcontracting

But it remains difficult to keep tabs on where commodities are sourced in supply chains. Distelhorst and de Zegher don't believe technology alone can ensure responsible sourcing practices. It requires companies contracting with suppliers to enforce penalties for irresponsible behavior and foster relationships that encourage ethical action.

Many times, issues along a supply chain begin when a supplier is feeling pressured to maintain a lucrative relationship with a big-name brand. If they take on too many orders to try to keep the client happy, they find that they need to subcontract some of the work out to stay on schedule. Those subcontractors may not adhere to the same labor standards.

"You're left with a choice: Should I tell this wonderful customer that I can't manufacture that right now because I have too many orders in the plant, or that I can manufacture it but it'll be weeks later, or, alternatively, subcontract that out to some factory that your customer does not know about. It's the unauthorized subcontracting problem," Distelhorst said.

If the penalties for taking that route are weaker than the penalties for shipping an order late, there's a higher incentive to engage in unauthorized subcontracting. Eliminating those incentives will require harder policing by buyers, with higher penalties around that sort of behavior.

But a company's ability to penalize a supplier is limited to the extent that it does business with them. Apple, for example, is considered a global leader in pursuing a more humane supply chain because the company has invested in improving its information sensing capabilities, Distelhorst said, expanding their ability to use third-party auditors to inspect the smelters deep in their supply chain.

"That's a significant accomplishment. Not only does Apple not own those smelters, it's also very likely that they're not doing any direct transactions with those enterprises," he said. "These are smelters that are selling to their subcontractors, and those subcontractors are then selling the product."

But, not every company is as huge as Apple. Smaller companies will have less power to enforce penalties on suppliers. Even Apple is unable to know absolutely everything about its own chain. Just look at the Congolese cobalt case.

15%

Noncompliance with labor standards was reduced by 15% when Nike implemented lean practices in factories.

Try lean manufacturing

Recent research from Distelhorst demonstrates suppliers that adopt lean manufacturing can improve efficiency while improving working standards. This method aims to eliminate waste in production lines without sacrificing productivity. It typically involves expanding a worker's role to include a wider range of tasks.

"We have a few examples where there are interventions you can do in factories that simultaneously improve the productivity and seem to result in better working conditions," Distelhorst said, with Nike being the most visible.

When Nike implemented lean manufacturing in factories in its supply chain to improve their efficiency, those factories saw a 15 percent reduction in noncompliance with labor standards such as wages, benefits, and time off. He believes that's because lean encourages workers to engage in more complex tasks, which makes them more important to train and retain.

"What was really appealing about that intervention was that it was not seen as an intervention that was policing them and creating higher penalties for not complying — it was seen as coaching those factories around a new production system," Distelhorst said.

Implementing this requires a high level of trust between the buyer and the supplier. A buyer can encourage lean manufacturing but won't suffer significantly if it doesn't work out. "If that factory owner doesn't trust you to have their interests at heart, they're going to be very skeptical of making any changes," Distelhorst said.

A relationship also needs to be long-term in order for a supplier to be receptive to adopting a new, more ethical way of doing business.

> *"Often, reducing harm in the supply chain is complex, and it therefore requires time and long-term engagement between buyers and suppliers."*
>
> **Joann de Zegher** | MIT Sloan

Stick with it and effect change

When facing intense public pressure when something goes wrong in its supply chain, companies find themselves tempted to sever ties with a supplier to satisfy the outcry.

But de Zegher said that could do more harm than good. In the Congolese cobalt case, miners rely on the industry to power their local economy, despite the clear dangers of the work. When buyers stop doing business in the area, the miners may find themselves without any source of income.

"Often, reducing harm in the supply chain is complex, and it therefore requires time and long-term engagements between buyers and suppliers," de Zegher said. "When a company gets slammed by a media campaign, it may find that it is too challenging to explain this complexity to the public, and it has no choice but to shut down relationships with the suppliers — just to be able to send a clear signal to the public. This can lead to significant back-tracking of progress and comes with the risk that the supplier is forced back to poor practices or worse."

Distelhorst said public campaigns against issues deep in a company's supply chain that force such action also disrupt a company's ability to provide products to its customers by cutting off its ability to source the materials needed.

"[A buyer] just literally cannot do business with them anymore without suffering severe reputational damage," he said. "As successful as Nike's been over the last few years, that shadow really hangs over them from the 1990s, even as Nike has made great progress and become an innovator in responsible supply chain management."

SHUTTERSTOCK / YURCHANKA SIARHEI

Blockchain for business starts in the supply chain

by **Tam Harbert**

Why It Matters

Crypto hogs the headlines, but supply chains are more likely to be blockchain's first practical use case, MIT experts say. Here's how to proceed.

WILL BLOCKCHAIN DISRUPT YOUR INDUSTRY? Maybe, but it's not likely to happen anytime soon. At least that's the opinion of many MIT experts who watch the blockchain space.

"[Right now] the actual live use cases of blockchain are predominantly for speculative investing," said MIT Sloan professor Gary Gensler, a senior advisor to the MIT Digital Currency Initiative and former chairman of the U.S. Commodity Futures Trading Commission.

Michael Casey, senior advisor to the Digital Currency Initiative, agreed. "Across the board, actual productive use of blockchain for day-to-day business operations is still extremely thin. There's no doubt about that," said Casey, co-author of "The Truth Machine: The Blockchain and the Future of Everything."

Neha Narula, director of the initiative, may have summed it up best as she moderated a panel at MIT's 2019 Business of Blockchain conference. Referring to MIT's first blockchain conference three years earlier, Narula said, "Maybe in 2016 we underestimated the amount of learning that needed to happen at all layers."

Blockchain is a distributed ledger technology that creates an unchangeable record of transactions, facilitating interaction between participants without the need for intermediaries such as banks.

The technology is complex and not conclusively defined — some so-called blockchain applications are simply traditional distributed ledgers, lacking blockchain's hallmark features of anonymity and immutability, experts have pointed out. What's more, figuring out how and when to apply blockchain is challenging, and companies are struggling with the business model.

> *Blockchain is a 'we' technology, not a 'me' technology.*
>
> **Michael Casey** | MIT Sloan

"We are on a giant, giant learning curve right now," said Simon Whitehouse, senior managing director for financial services, growth, and strategy at Accenture, who also spoke at the conference. Most companies don't yet understand "how blockchain can work, how it can add value, and why they have to cooperate and compete with partners at the same time."

Different consortia have formed in different industries to try to collaborate on blockchain, but progress has been limited. "The reason it's taking such a long time is not necessarily a technical problem," said Casey. "It is a cultural and structural challenge getting different non-trusting parties to work together. Blockchain is a 'we' technology, not a 'me' technology." Its biggest benefits are for the group, not a single company.

First up: supply chains

Although the initial enthusiasm was about finance, supply chains are more likely to be the first real, practical use case for the technology, said Irving Wladawsky-Berger, a visiting lecturer at the MIT Sloan School of Management.

"Financial systems are among the most ungodly complicated systems you can imagine," he said, making the application of a complex technology like blockchain extra difficult. Supply chain applications can be simpler, and the potential value more straightforward.

Wladawsky-Berger said he can explain a supply chain application in the time it takes to deliver an elevator pitch, albeit a longish one (30 floors, he said). "If you are going to develop something complicated, being able to describe it simply is very important," he said. "I think that's a major part of why supply chain is the killer app of blockchain."

As a shared digital ledger that creates an immutable record of transactions, blockchain is ideal for tracking the provenance of goods. It enables trustworthy shared information among suppliers that may not trust each other. "One of the best ways to think about blockchain is in the context of a supply chain," said Casey. It enables a group of independent entities, which have their own interests and information to protect, to share a common platform that holds information of common interest.

> *Supply chain is the killer app of blockchain.*
>
> **Irving Wladawsky-Berger** | MIT Sloan

It helps to have a dominant company driving the use of blockchain, as is the case in two supply chain applications that may be close to going into production. Walmart has been running a pilot project with IBM's Food Trust Solution, a blockchain-enabled distributed ledger of food system data, to track lettuce from its suppliers to Walmart shelves.

And Dutch shipping company A.P. Møller-Maersk is using IBM technology in a blockchain pilot that will track ocean cargo containers. Five of the world's largest carriers, controlling a majority of container cargo capacity, have signed on, according to the Wall Street Journal.

Finance and cryptocurrencies

There are plenty of potential uses in finance — using blockchain to control and service loans or underpin smart contracts, for example. But for now at least, the lion's share of attention is going to cryptocurrencies and stablecoins, said Gensler, who with Narula co-teaches an online course on cryptocurrency.

Cryptocurrencies like Bitcoin and Ethereum are a form of private digital cur-

> *We're still in early years with this whole thing.*
>
> **Gary Gensler** | MIT Sloan

rency that use cryptography and blockchain to secure and verify transactions. Stable value coins like Tether, USD Coin, and proposed offerings from Facebook, JPMorgan Chase, and Deutsche Bank are pegged to currency or another asset so that they are less volatile than a cryptocurrency.

Further, several central banks are creating their own tokens. The tiny Republic of the Marshall Islands (population: 53,000) has launched the Marshallese sovereign (SOV), while the People's Bank of China is reportedly planning to issue its own digital currency.

It's not clear that any such alternative payments would be better than the current digital distributed ledger technology and digital payment structure that banks already use to move money, Gensler said. The United States, for example, uses the Automated Clearing House, among others, and it works well. "Shared distributed ledgers have been around for decades. Blockchain technology is not new in that regard," Gensler said.

Although there are more potential use cases than real ones for blockchain in business, that could change fast. "We're still in early years with this whole thing," Gensler cautioned. "Where we'll be in 2025 or 2030 is yet to be known."

Building up to blockchain

As business leaders watch developments in (and hear the hype about) blockchain technology, they can stay grounded by asking practical questions about what blockchain can and cannot do for their organizations, the experts advised.

Start by asking strategic questions, said Gensler. "These big strategic questions aren't hard to ask," said Gensler, but they can be hard to answer, which is where their value lies. Among them:

- **What's the value proposition? What problem will this solve, and how will blockchain be better than other solutions?**
- **More specifically, blockchain is by design immutable — meaning once it's been added, data in the blockchain cannot be altered. Does your application need that?**

Gensler also suggests these tactical questions:

- **What data will be written to the ledger?**
- **Who (within a company) will be allowed to write to the ledger?**
- **Who (within a company) will be allowed to see the ledger?**
- **How will the parties preserve confidentiality of data and comply with privacy laws?**

The biggest challenge for blockchain applications is the extent to which companies will truly collaborate, according to Casey. In a consortium of equals, when there is no dominant player "to bash all the heads together and make them do it," what is the motivation for companies to participate, he asked. Projects that deliver valued outcomes to all parties are more likely to succeed.

If you decide to explore blockchain, start small, then grow incrementally as you learn about the technology and convince other companies to work with you, said Wladawsky-Berger. "Don't swing for the fences," he said. "Just get on base."

ILLUSTRATION: ROB DOBI

Supply chain visibility boosts consumer trust, and even sales

by **Sara Brown**

Why It Matters

Investing in supply chain transparency can be costly. But companies making the investment earn points with consumers, and even higher sales from socially conscious or skeptical buyers.

GLOBAL SUPPLY CHAINS ARE COMPLEX. Transforming raw materials into completed goods often requires a multitude of workers crossing different countries and cultures. Companies undertaking efforts to learn more about their supply chain often face a significant investment of time and resources.

Those costs are worth it, according to a new study by MIT Sloan professor Y. Karen Zheng and visiting assistant professor Tim Kraft along with León Valdés, an assistant professor at the University of Pittsburgh.

The researchers found that investing in supply chain visibility is a surefire way for companies to gain consumer trust and can even lead to increased sales from certain customers.

"Increasing supply chain visibility always strengthens consumer trust," the researchers write. "Furthermore, opportunities exist for a trust-driven revenue benefit due to greater visibility

Common elements of supply chain visibility include tracing parts or products along every step of the manufacturing process, from raw materials all the way to the final product being delivered to the consumer, and finding out more about factors including working conditions and environmental impact.

Zheng, Kraft, and Valdés arrived at this conclusion after conducting a study with 467 participants at two U.S. universities. The participants played a game with three roles that mimicked a supply chain: a consumer, a seller, and a disadvantaged worker. Within the game the seller had to decide how much to invest in supply chain visibility, and whether to communicate that information to the buyer, truthfully or not. Consumers then had to decide whether or not they believed the seller and whether to buy the product. The decisions were monetarily incentivized.

The researchers also ran control tasks that gauged the participants' levels of risk preference, trust beliefs, and prosociality — willingness to sacrifice something to one's own benefit to increase another person's payoff.

Here are the key takeaways.

Supply chain visibility is a surefire way to gain trust

Consumers are caring more about a company's social responsibility. According to a recent poll referenced by the researchers, 75% of respondents considered transparency helpful in strengthening trust between businesses and consumers. But few companies invest in learning more about supply chain visibility, which allows for transparency with consumers. According to another poll cited by researchers, 81% of 1,700 companies surveyed did not have full visibility into their supply chains, and 54% had no visibility at all.

Researchers said that in all versions of their experiment and no matter the player's prosociality or other preferences, improving visibility increased consumer trust in a company's communication about social responsibility.

Even though transparency is expensive, risky, and time-consuming, the study found, investing in supply chain visibility is an important tool to strengthen consumer trust. "At a time when customers are becoming savvier — and more skeptical — about social responsibility, our findings show that the investment can be worthwhile as it always engenders consumer trust," Kraft said.

Consumer trust goes up even more as the economic status of workers in the supply chain decreases. "For companies that source from suppliers in developing countries where workers live in potentially poor economic conditions, there is an even stronger potential benefit from investing to improve supply chain visibility," according to the researchers.

54%

Percent of companies surveyed had no visibility into their supply chain.

More visibility means more sales from some consumers

Increased consumer trust has its own benefits, including increased customer loyalty and brand recognition. Researchers found that among some consumers more trust also leads to increased sales.

It depends on the company's consumers. Supply chain visibility matters most to consumers who value philanthropy and are empathetic to others' well-being and to those who tend to be naturally skeptical. In those cases, sharing information about the supply chain overcomes consumers' inherent lack of trust or makes prosocial customers feel like they are patronizing a socially responsible company.

Even small social responsibility initiatives make a difference

Taking even small actions based on increased supply chain visibility can pay off, according to the study.

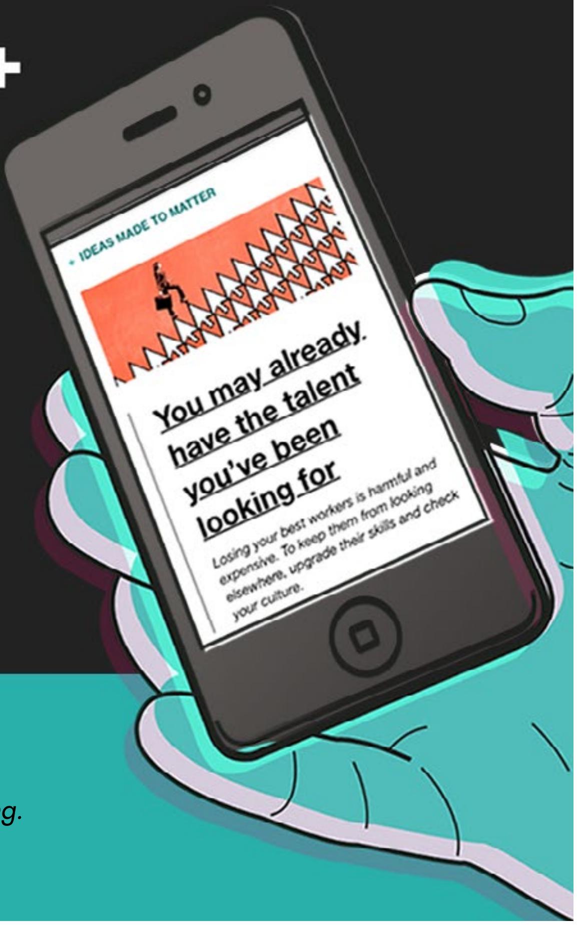
Initiatives based on great visibility that offer even a small impact, like slightly increasing pay for workers, are likely to boost trust-driven sales. "This is because investing in visibility mitigates skepticism and prevents consumers from punishing the company (i.e., not purchasing the product) due to the small impact of the [social responsibility] initiative," the researchers write.

"Customers want to know more about where and how the products they purchase are made," Zheng said. "And even small investments in supply chain visibility can make a big difference for a company."

THINKING+++ FORWARD

Want more Ideas Made to Matter?

Sign up for our Thinking Forward newsletter.



‹ IDEAS MADE TO MATTER

You may already have the talent you've been looking for

Losing your best workers is harmful and expensive. To keep them from looking elsewhere, upgrade their skills and check your culture.

SIGN UP HERE

mitsloan.mit.edu/thinking-forward

Insights from MIT experts, delivered every Tuesday morning.

MIT Sloan Office of Communications
Building E90, 9th Floor
1 Main Street, Cambridge, MA 02142

Questions and Comments: thinkingforward@mit.edu
mitsloan.mit.edu

MIT MANAGEMENT SLOAN SCHOOL | IDEAS MADE TO MATTER