Safeguarding trust in a digital ecosystem

Marcos Aguiar, Jeff Kiderman, Harsha Chandra Shekar and Oliver Schilke

Introduction

A mere four years after its founding, Airbnb was operating in 89 countries and had just become a Silicon Valley unicorn. Then came a raft of property-trashing incidents. In response, the company radically upped its host-property guarantee to $1m. Since then, with every new form of mishap, transgression or breach, whether by hosts or guests, Airbnb has steadily amended or expanded its safeguards (including age restrictions, identity checks and reviews) and its ground rules (which are designed to ensure fair play and accountability and offer recourse for repeat offenders).

Consider the converse: In Uber's early days, to fend off mounting competition from Lyft and to grow the business faster, the company saw the need to expand capacity and lower prices. To attract more drivers, the company waived the commercial driver's license requirement. Although controversial at the time, relaxing this safeguard transformed the shape of urban mobility.

Safeguards are meant to protect either or both sides of a transaction or interaction in an online ecosystem and reduce negative outcomes. Too few can hinder an ecosystem's growth. Yet too many can be time consuming and costly to maintain and potentially intrusive, stifling relationships and other positive outcomes that spring from a free-market exchange.

So how do companies know when their safeguards are too onerous? How many are too many? Conversely, how can companies tell when there are not enough? In designing safeguards, ecosystem orchestrators must find a sweet spot. Because trust is at the heart of digital interactions and ecosystem success, safeguards should be the concern not only of operations but also of orchestrators and participants.

What exactly are safeguards?

Safeguards refer to the precautionary mechanisms that an ecosystem relies on to mandate or promote desirable behavior and engender trust among its participants (Hill, 1990; Luhmann, 1979; Zhang *et al.*, 2022). There are many types of safeguards – including policies, practices and tools – and multiple types can be used to address the same concern. Safeguards may include hardware, software and human-enabled mechanisms. For example:

- escrow and blockchain mechanisms that aim to foster transparency in a transaction;
- identity verification tools, such as passwords, biometrics and multifactor authentication;
- data controls that allow users to monitor or get information about counterparties and that protect users' privacy;
- digital reputation tools – including ratings, reviews and awards – that serve as signals about sellers' behavior and integrity;
- constraints, such as policies, sanctions and contracts.

Marcos Aguiar, Jeff Kiderman and Harsha Chandra Shekar are all based at the Boston Consulting Group, Boston, Massachusetts, USA. Oliver Schilke is based at the Department of Management and Organizations, Eller College of Management, The University of Arizona, Tucson, Arizona, USA and Department of Sociology, The University of Arizona, Tucson, Arizona, USA.

Research support was provided by a National Science Foundation CAREER Award (1943688) granted to Oliver Schilke.

Safeguards do their work at many junctures in the user journey. Depending on their type, they get baked into operating models, the user experience, marketing practices and software and payment systems, for example.

Advanced digital technologies have opened the door to new types of safeguards and their unprecedented usage (Evans *et al.*, 2021), which will only continue to grow. AI-driven algorithms, for example, are frequently used to identify and block fraudulent transactions (Lumineau *et al.*, 2023). Although the scalability of these technologies makes them powerful tools, ecosystem leaders need to actively gauge their true impact (individually and in aggregate) in amplifying, neutralizing or diminishing the desired behaviors.

Why are safeguards mission critical?

Safeguards are ultimately about generating trust (Bachmann and Inkpen, 2011), and virtually every ecosystem – whether it is Alibaba or Etsy, Lyft or DoorDash, Google Play Store or Apple's App Store, Airbnb or TrustedHousesitters – depends critically on trust (Shipilov and Gawer, 2020). With the rise of ecosystems, and as digital interactions increasingly replace interpersonal dealings, trust has become a vital currency for economic success – the element that greases the wheels of an ecosystem, allowing it to scale. In fact, a recent study shows that among successful ecosystems, 86% had actively embedded trust mechanisms (of which safeguards are the lion's share) into their ecosystems and practices (Aguiar *et al.*, 2021). An orchestrator cannot build an ecosystem and hope that trust will emerge spontaneously among strangers. An orchestrator has to design for trust (Altman *et al.*, 2022; Chen *et al.*, 2002).

Importantly, safeguards enable actions and engagement by providing reassurances that participants can trust the ecosystem even if they lack experience with (and have not developed trust organically with) the counterparty (Schilke and Cook, 2015). Safeguards help align expectations about processes and outcomes, thus reducing the uncertainty about the counterparty's behavior (Cao and Lumineau, 2015). They also provide economic incentives for a partner to behave in a trustworthy fashion. In this way, safeguards foster trust in the overall ecosystem – what we deem as systemic trust – making trust between counterparties less crucial. Yet well-designed safeguards can also work to foster relational trust – trust between two parties – not just systemic trust.

Are more safeguards always better?

An under-reliance on safeguards raises the risk of undesirable behavior, negative outcomes and even friction. Friction is anything that makes participants wait or hesitate to act or that causes confusion or frustration. Uber Eats, for example, recently discovered that many restaurants were listing multiple brands on the platform with the same menu – brands coming from online (virtual) storefronts. Customers were thus seeing dozens of versions of the same menu on the app, which made searches annoying. Such friction can lead to churn or, worse, failure.

On the contrary, an excess of safeguards can stifle the interactions that make trust flourish organically among participants and that spark innovation, creativity and other often unexpected benefits. In addition, too many safeguards almost always come at a cost. Apart from the direct costs involved in implementation and enforcement, an excess of safeguards can make the user experience more frustrating, bureaucratic and generally less enjoyable. An overabundance of safeguards can also make participants suspicious; they wonder why there are so many constraints. That reaction undermines the very purpose of safeguards. As a result, participants may become circumspect, less loyal and more likely to go elsewhere.

The trick for ecosystem orchestrators is to strike the right balance between control and autonomy. The right balance depends on several factors, including the ecosystem's purpose, participants' characteristics, the nature of the goods or services being bought and sold and how high the stakes are. For instance, a marketplace offering handcrafted artistic goods may reasonably require each seller to provide a variety of unique high-quality product images, whereas an e-retailer selling commoditized goods may allow generic images. A platform for long-term housing rentals may require a credit score check on prospective tenants, whereas such a safeguard may not be necessary for one that rents vacation homes short-term.

Whether to err on the side of having more or fewer safeguards can be one of an orchestrator's most challenging and consequential design decisions. To illustrate, an orchestrator of a peer-to-peer marketplace might consider asking these questions:

- Should sellers be able to sell whatever they want? Should the company verify that the sellers own the products they are selling or document sellers' credentials?
- Should sellers be able to set their own terms for pricing? Should buyers be allowed to negotiate the price?
- Should sellers be able to take as long as they want to deliver purchased items?
- Should buyers have full access to sellers' contact information?
- What are the return limitations for buyers?
- Should the company release payment when a seller indicates that an item has been shipped or when the buyer acknowledges receipt?

These decisions do not apply to just retail ecosystems; every ecosystem orchestrator, whether managing relationships between hosts and guests, artists and patron, or any other set of counterparties, has hundreds of decisions to make along these lines.

What factors should orchestrators consider?

When deciding which safeguards an ecosystem needs and what constitutes the optimal mix, an orchestrator should consider a number of parameters (see Figure 1).

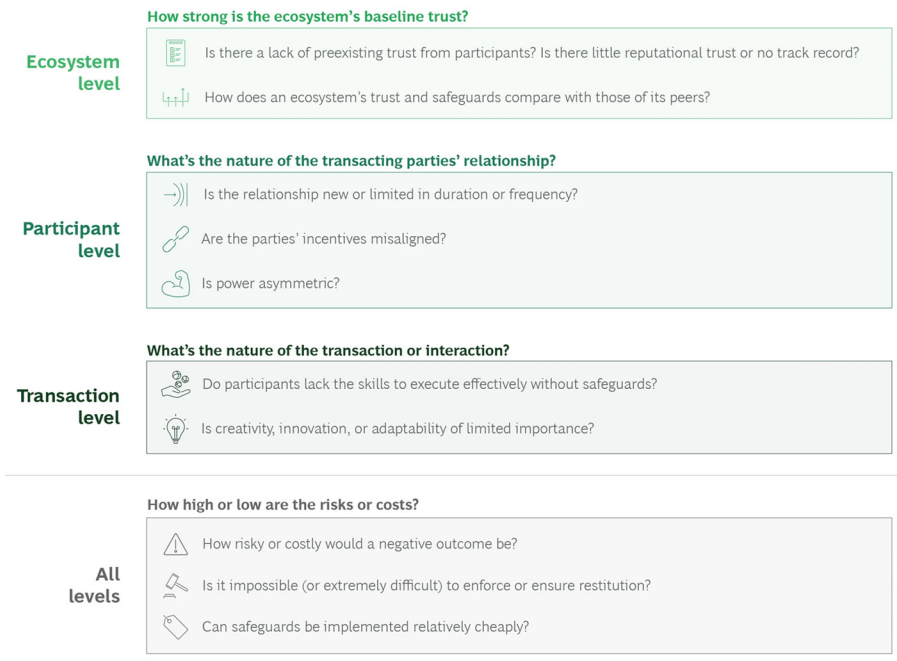
Here, we will focus on what we believe are the most critical ones:

Power asymmetry between a seller and buyer

A classic example of a safeguard to address asymmetric power is the use of escrow: a marketplace orchestrator withholds payment to sellers (especially new ones) until they submit proof of shipment. Another is offering a guarantee to buyers, such as a 30-day free-return policy, or imposing a penalty on sellers who do not adhere to the ecosystem's policies and practices. In addition to transaction-oriented power asymmetry, there is the innate relationship-oriented type. An orchestrator needs to serve as a regulator for both kinds of power asymmetry, ensuring that the more powerful actors do not abuse their natural advantage.

In contrast, when power dynamics are less one-sided, fewer safeguards are typically needed and may be counterproductive. For Uber and Lyft, for example, general contracting checks (that determine whether a driver has a good driving record, for example) and customer reviews do a fairly good job of ensuring appropriate behavior. The auction site uShip, which connects those seeking discounted shipping services with carriers (chiefly truckers wanting to avoid deadheading), provides basic tools (including listings, policies, a messaging center and profiles) along with optional tools (a tracking app, for example) and suggestions for both parties (such as creating a written agreement using their template).

Figure 1 How to choose safeguards in an online ecosystem



Source: Boston Consulting Group Henderson Institute

Sophistication or skill level of participants

More safeguards may be warranted for ecosystems that eliminate intermediaries, that have more technically or legally complicated transactions, and whose users have relatively little experience. Consider ecosystems where real estate is sold by owners. The risk for participants is not necessarily about encountering unscrupulous counterparties. It is more about both parties – nonprofessionals – making mistakes in a deal as complex as a house purchase. Some do-it-yourself real estate ecosystems work with third parties to offer safeguards such as documentation reviews and process assistance. Platforms where participants buy and sell heavy equipment are another example of ecosystems that may need more safeguards, because such sales have traditionally involved brokers or distributors.

When most participants in an ecosystem have the necessary skills or knowledge to understand key aspects of a transaction, safeguards tend to be less critical. In fact, for participants with advanced skills, too many safeguards bureaucratize a process, adding unnecessary complications, not to mention increasing costs. Consider a commercial real estate platform designed for professionals. Too much red tape could cause deals to drag out, potentially causing one or both parties to lose an opportunity or possibly risking a change in transaction costs if interest rates or market prices fluctuate.

The nature of the transaction

When creativity is central to the ecosystem's purpose, less may be more when it comes to safeguards. Patreon connects patrons and creators of all types, including visual artists, writers, videographers and humorists. Rather than buy a specific product, users subscribe to receive content from creators. There are relatively few safeguards surrounding these offerings, allowing Patreon's 250,000 creators the freedom to design their own packages of content and pricing tiers. Creative content is, after all, not a commodity, and even for a

single creator, the time it takes to produce art – a sketch versus a series, or a song as opposed to a sonata – can vary greatly.

Art is one thing; technology is another. As an open-source operating system, Linux needs to encourage innovation. But because major institutions and businesses worldwide depend on the system, some safeguarding is in order. A hierarchy of code maintainers ensure integrity by evaluating input from contributing developers. This modest counterbalancing safeguard ensures that the platform allows for creativity and collaboration among the thousands of developers in its community.

The cost of a negative outcome

When the stakes are relatively low, or a negative outcome is relatively easy to fix, there is less of a need for stringent safeguards. A food delivery app, for example, may guarantee only the price or the speed of delivery, not the quality of meals from its restaurant purveyors. And to exercise that guarantee, a user must take the time to submit a complaint and await the company's reply, an effort that many would deem too great to recoup a modest difference in meal cost or be compensated for a longer wait. A platform selling vintage knickknacks or handmade costume jewelry may not require an upfront proof of provenance; the ability to return for a refund is all that a disappointed customer would expect with such goods.

But with a high-stakes interaction or transaction, more (or more stringent) safeguards tend to be better. A marketplace specializing in antique estate jewelry or rare manuscripts would likely require documented expert authentication of each item to protect buyers. HopSkipDrive, a ride service designed to transport unescorted kids, provides multifactor authentication upon pickup to ensure that kids and drivers find each other safely. In addition, a real-time tracker allows parents to trace the location of the car transporting their child while it is in transit. Background checks for drivers are considerably more rigorous than for other ride-hailing services. Despite the fact that the checks may scare off some potential drivers, thus hindering the ecosystem's growth, such robust safeguards are vital for engendering the trust of customers under such circumstances.

Buying a car online at eBay is a far bigger gamble than buying a steering wheel cover or replacement headlights. eBay Motors and most other online auto marketplaces offer free Carfax reports on each vehicle's history. eBay's vehicle protection program covers buyers up to $100,000 and protects against such risks as not receiving the title (or the car itself), an undisclosed lien and unknowingly purchasing a stolen vehicle.

The cost-benefit tradeoff

Whether it is dispute-resolution mechanisms or authenticity-verification tools, implementing and maintaining safeguards may not be cheap. Ecosystems often operate on slim unit economics (often earned as a percentage of each transaction's value), so it is usually unfeasible to support extensive safeguards. Orchestrators, therefore, need to weigh the cost-benefit tradeoffs.

It is also impracticable for a massive online marketplace, such as Amazon or Alibaba, to inspect vendors' wares before they are shipped to customers. The user rating system substitutes reasonably well (albeit not perfectly); it is a marginal cost for an orchestrator, yet offers an easy and valuable solution for buyers and sellers. Still, there are many cases in which the stakes are high and the benefits justify the costs. Uber and Lyft, for example, need to ensure that their drivers are licensed and insured; the failure to do so can result in significant fines, liability, regulatory action and bad press.

Competition and change make adapting safeguards essential

Implementing safeguards is not a one-and-done exercise. Changes in an industry, a user base, technology or an ecosystem's business model (Wirtz *et al.*, 2010) or strategy make it

imperative to continuously monitor and adapt safeguards. But change is not always gradual. A disruptive innovation or major breach that harms participants and the ecosystem itself may trigger the need to modify safeguards drastically.

Many of the safeguard adjustments that Elon Musk has instituted at Twitter since buying the company – loosening restrictions in some areas and clamping down in others – illustrate the delicate balancing act that managing safeguards can be, particularly in social media.

Competitive pressures may also need to influence safeguard decisions, especially in an increasingly winner take most (if not all) world. Uber relaxed its initial requirement of a commercial driver's license to match Lyft's less stringent one. Safeguards can also be a means of strategic differentiation; Google, for example, opted for fewer safeguards for its app developer ecosystem than did Apple.

Implementing and adjusting safeguards

How does an ecosystem orchestrator apply parameters in practice to achieve the right balance between control and freedom? First, consider the ecosystem as a whole. Identify which two or three parameters shown in Figure 1 appear to best define the need for safeguards – or their downside. In addition to the parameters we have described already, others include the ecosystem's preexisting reputation and track record and the typical nature or maturity of participant relationships.

Then, break down the ecosystem into value streams of participants' experiences to pinpoint where more or fewer safeguards would be useful. For drivers of a ride service, for example, identify the various stages of their experience, including signing up, passing a background check, onboarding, setting up a payment method, receiving reviews and resolving problems.

What happens when parameters conflict? Say the need for creativity (and thus, fewer safeguards) is high, but the cost of a negative outcome is also high. In that case, dig down to a more granular level to isolate the value stream activity with a high need for creativity and the activity with a high level of criticality. If they cannot be separated, prioritize using safeguards in a way that benefits the critical aspects of the activity without hindering its creative aspects.

After establishing and prioritizing the trust issues, identify the appropriate safeguard or safeguards that are needed. Choose metrics to gauge safeguard balance – both the overall balance and that of high-priority elements. Then, monitor, test and iterate as needed. Due diligence will be an ongoing exercise of pulling back and pushing forward to maintain that delicate balance of freedom and control.

With the right mix and the right number, safeguards are a key to an ecosystem's health and growth. They are not merely elements of the operating model; they are also central elements of the ecosystem's value proposition and its competitive advantage. So, finding the sweet spot between control and autonomy, risk and reward, is crucial. It requires constant vigilance and tweaking, as the competitive landscape, technology and user expectations evolve – or get disrupted (Christensen, 1997; Schilke, 2014). In nature, adaptation is everything. So it is with digital ecosystems and their safeguards.

Keywords:
Trust,
Safeguards,
Organizational design,
Constraints,
Ecosystems

References

Aguiar, M., Pidun, U., Lacanna, S., Knust, N., Williams, M. and Candelon, F. (2021), "Discovering the tools and tactics of trust in business ecosystems", available at: www.bcg.com/publications/2021/building-trust-with-stakeholders-in-business-ecosystems (accessed 31 July 2023).

Altman, E.J., Nagle, F. and Tushman, M.L. (2022), "The translucent hand of managed ecosystems: engaging communities for value creation and capture", *Academy of Management Annals*, Vol. 16 No. 1, pp. 70-101.

Bachmann, R. and Inkpen, A.C. (2011), "Understanding institutional-based trust building processes in inter-organizational relationships", *Organization Studies*, Vol. 32 No. 2, pp. 281-301.

Cao, Z. and Lumineau, F. (2015), "Revisiting the interplay between contractual and relational governance: a qualitative and meta-analytic investigation", *Journal of Operations Management*, Vols 33/34 No. 1, pp. 15-42.

Chen, L., Tong, T.W., Tang, S. and Han, N. (2022), "Governance and design of digital platforms: a review and future research directions on a meta-organization", *Journal of Management*, Vol. 48 No. 1, pp. 147-184.

Christensen, C.M. (1997), *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, MA.

Evans, P., Aguiar, M., Williams, M. and Lacanna, S. (2021), "Beyond blockchain: the promise of digital trust networks", available at: www.bcg.com/publications/2021/digital-trust-networks-promises-digital-trust (accessed 31 July 2023).

Hill, C.W.L. (1990), "Cooperation, opportunism, and the invisible hand: implications for transaction cost theory", *Academy of Management Review*, Vol. 15 No. 3, pp. 500-513.

Luhmann, N. (1979), *Trust and Power*, Wiley, Chichester.

Lumineau, F., Schilke, O. and Wang, W. (2023), "Organizational trust in the age of the fourth industrial revolution: shifts in the nature, production, and targets of trust", *Journal of Management Inquiry*, Vol. 32 No. 1, pp. 21-34.

Schilke, O. (2014), "On the contingent value of dynamic capabilities for competitive advantage: the nonlinear moderating effect of environmental dynamism", *Strategic Management Journal*, Vol. 35 No. 2, pp. 179-203.

Schilke, O. and Cook, K.S. (2015), "Sources of alliance partner trustworthiness: integrating calculative and relational perspectives", *Strategic Management Journal*, Vol. 36 No. 2, pp. 276-297.

Shipilov, A. and Gawer, A. (2020), "Integrating research on interorganizational networks and ecosystems", *Academy of Management Annals*, Vol. 14 No. 1, pp. 92-121.

Wirtz, B.W., Schilke, O. and Ullrich, S. (2010), "Strategic development of business models: implications of the web 2.0 for creating value on the internet", *Long Range Planning*, Vol. 43 Nos 2/3, pp. 272-290.

Zhang, Y., Li, J. and Tong, T.W. (2022), "Platform governance matters: how platform gatekeeping affects knowledge sharing among complementors", *Strategic Management Journal*, Vol. 43 No. 3, pp. 599-626.

About the authors

Marcos Aguiar is a Managing Director and Senior Partner at Boston Consulting Group, São Paulo, Brazil. He is a BCG Henderson Institute Fellow and a senior member of the Industrial Goods, Metals and Mining, Technology, Media and Telecommunications, People and Organization, Strategy, and Global Advantage practices. He leads the firm's global work in Brazil insights and agenda-setting.

Jeff Kiderman is a Principal at Boston Consulting Group, Washington, DC and a BCG Henderson Institute Ambassador.

Harsha Chandra Shekar is a Partner Boston Consulting Group, Seattle, Washington.

Oliver Schilke is a Professor of Management and Organizations and the Director of the Center for Trust Studies, Eller College of Management, University of Arizona, Tucson, Arizona. This research was conducted in part while he has served a Distinguished Visiting Faculty at Tecnologico De Monterrey - EGADE Business School. Oliver Schilke is the corresponding author and can be contacted at: oschilke@arizona.edu