The 11 Principles of Trust

How to Create Business Value Through Trust

GeorgianPartners

Why Trust Matters

When data is the lifeblood of your business, it's critical that customers, partners and regulators trust you to protect their information. Trust is a universal concept that applies not only to people, places and things, but also to companies, products and services across all industries.

Are there any software companies that you would voluntarily trust to protect your most intimate personal details? Do you trust them because you believe they'll do everything in their power to protect your information or simply because their services are so integral to your life that you feel you have no other choice? Unfortunately, many of us have resigned ourselves to sharing data even though we feel increasingly uncomfortable about it.

Trust is particularly important for software companies that build products using machine learning and artificial intelligence (AI). It allows companies to access the data that they need to fuel models and ultimately power AI solutions. However, AI also presents new challenges for trust. Since much of the data that companies use to train AI is generated by humans who are often themselves biased along racial, gender or other lines, there's a risk that this bias can become embedded in an AI model and propagated at scale. In addition, as AI techniques become increasingly complex, companies will need to figure out how to explain the choices of their models instead of simply assuming that users are happy to trust a black box.

We believe that this current state of affairs presents a clear opportunity for software vendors to differentiate on trust. Companies that emerge as trust leaders will be able to drive the discussion on how data should be collected, created, used and protected in their ecosystems over the coming years. As a result, their customers will share more data, use more services, and become less likely to abandon their products. Thus, the degree to which customers trust your company, your products and your brand will directly impact your revenue, growth and sustainability.

The New Era of Trust

Software companies used to be implicitly trusted with customer data, but a wave of high-profile scandals has made governments, enterprises and consumers wary of sharing information at a time when companies need it more than ever to train models, extract insights and drive automation.

With that heightened awareness of data privacy issues, other aspects of software, including the business models themselves, are being scrutinized. We believe that customers will increasingly demand that companies operate fairly and transparently in how they treat customers, employees, and society as a whole.

More than ever, it's important for software companies to be proactive, to take opportunities to build trust competitively, and to challenge themselves to think how each action you take will increase or detract from your customers' trust.

Earning Trust

Trust is a careful balance between the value that you deliver and the comfort that customers experience when interacting with your company, brand and products. When these two factors come together, you get happy customers that keep coming back for more, and share their experiences with partners and friends. When they're decoupled, you may briefly enjoy success, but eventually trust will erode and customers will look elsewhere for greater value or comfort.

The matrix below helps visualize the balance between value and comfort. Companies in the top left deliver value; however, a security breach or a similar incident can materially impact customer retention, owing to a lack of comfort. In addition, companies in this quadrant can miss opportunities to acquire richer data from customers to enhance product capabilities. Companies in the lower right have a good reputation or a surplus of comfort that they can leverage to deliver more value and move to the top right. The risk is not acting on the opportunity in a timely manner and losing on value to their competitors.

Value / Comfort Matrix

Drivers of Value

Value is your core business proposition — the reason why customers are driven to adopt your product. Some of the most common ways that you might deliver value to customers are:[1]

- Improved top line
- Improved forecasting/analytics
- Improved product quality
- Cost and time savings
- Reduction of business risk
- Reduction of uncertainty, complexity and friction of doing business

Drivers of Comfort

Comfort is peace of mind for your customers — the understanding that accessing the value that you provide won't cause problems for them. Some of the most common aspects of comfort are:

- Reliability and stability
- Responsible and secure data handling
- Transparent business practices
- Customer control of data and influence on product direction
- Fair business model; shared vision and purpose

1 The B2B Elements of Value. Harvard Business Review. Eric Almquist, Jamie Cleghorn and Lori Sherer. March-April 2018. Accessed January 11, 2019.

From Security to Trust

As a thesis-based investment firm, we've chosen to focus on investing in companies that prioritize earning and safeguarding customer trust. This white paper is designed to help your company build a strategy to achieve just that.

Our trust principles represent an evolution of our thinking on Security First. Readers familiar with our principles of Security First will notice that there is continuity between the two sets of principles, and that our notion of trust covers a broader set of concepts.

How to Use This White Paper

This white paper introduces the principles of trust. In it, we also provide a framework for applying them to your organization, a maturity model that you can use to measure your progress toward trust, and a hypothetical case study to help put the ideas in context.

A Framework for Building Trust

The principles are grouped into six areas in the framework below. This shows how the components of trust relate to one another. The principles put these components into context to help you develop a trust strategy for your business.

Design

Design involves taking a proactive, strategic approach to trust. By designing a holistic trust program, you will have greater impact than pursuing a series of fragmented initiatives. Understand the needs of your market and prioritize your approach in your planning.

To operationalize your plans, create a roadmap for building trust and publish a set of values that reflect how your organization will use data. Set up a framework for accountability across the organization to make sure that your initiatives are accomplished. Review and iterate on your plans as expectations change.

Security

Security means protecting users' data from misuse or disclosure to internal and external threats. It is foundational to privacy and reliability. Build an effective security infrastructure before you collect your first piece of customer data. Putting off security improvements is simply another way of accruing technical debt, and a dangerous one at that.

Privacy

Privacy centers on giving customers control and oversight over how and where their data is stored, accessed, and used. Respecting privacy means understanding what users intend to share, with whom, and for what purpose, and then acting accordingly.

Fairness

Fairness means understanding the impact of your organization on groups and individuals and avoiding outcomes that are corrupt through bad design.

While technology has the power to greatly improve people's lives, it can also reinforce existing societal biases and unintentionally create new ones. Consider the unintended consequences of your organization on your users and other groups. Make your business model fair for all stakeholders and make efforts to reduce the impact of human bias.

Reliability

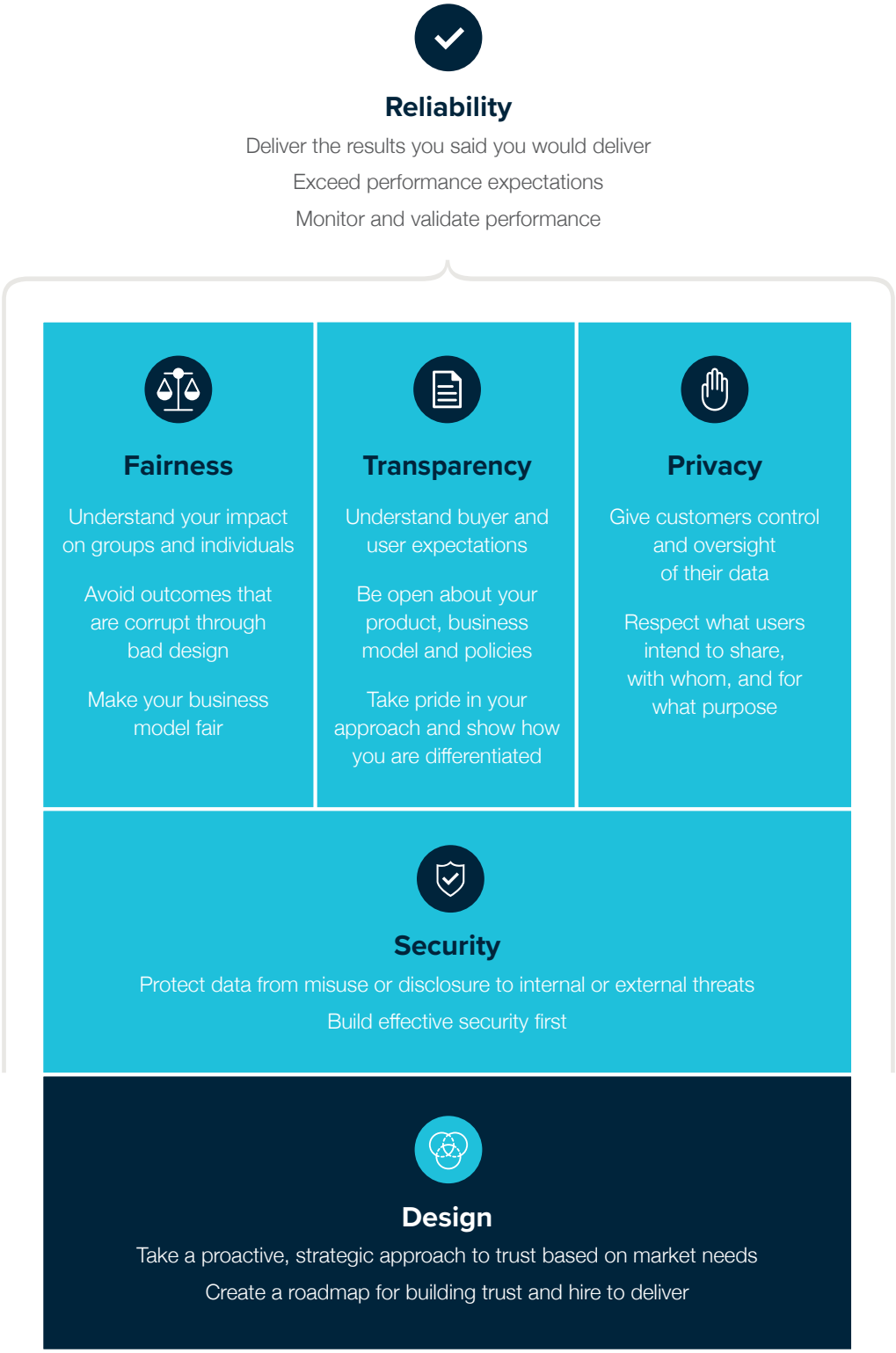
Reliability requires consistently delivering the results you said you would deliver to your customers. It's essential to understand (and meet or exceed) the performance expectations for your market by managing for any factors that could interrupt your business, such as errors, stability and bias.

Develop processes and controls to monitor and validate the performance of your systems and make sure that you have the knowledge and skills in your organization to predictably deliver value to your users.

Transparency

Transparency entails being open about your product, business model and policies, and explaining them in clear terms to users. This includes understanding user expectations and being prepared to describe your entire approach, from the choices you make in system and organizational design to the individual predictions of machine learning models. It's important to take pride in your approach to trust, and help customers understand how it differentiates you.

A Framework for Building Trust



Choose Your Strengths

Every company prioritizes different aspects of trust to meet market expectations. Your approach will be associated with your brand and will help your customers better understand your strengths across all areas of trust. Here are some examples of companies that have built their brand around different components of trust:

Design

Workday has designed its products, brand strategy and organization around trust, with executive roles and accountability supporting the trust function.

Security

BlackBerry rebuilt its reputation by focusing on secure endpoint management software.

Privacy

Apple took a leadership position on consumer privacy through taking a strong stance with law enforcement agencies.

Fairness

Google has dedicated significant resources toward building inclusive machine learning algorithms and conducting research on algorithmic bias.

Reliability

Amazon's reputation is built around reliability; customers trust that their items will be delivered on time, every time (and they're even willing to share the keys to their house).

Transparency

AT&T, LinkedIn, Twitter, Uber, Verizon and others publish regular transparency reports documenting the numbers and types of subpoenas, court orders and search warrants received from government agencies in different regions.

Multiple areas

Microsoft has a comprehensive approach to trust and has created its own Trust Center and Fairness, Accountability, Transparency, and Ethics in AI group.

Maturity Levels

Level 1

Capability and Ingredients

Your organization has intrinsic company characteristics, assets or strategic intent that give you an advantage for executing on trust. You have a basic understanding of priorities and opportunities, and there are few or no specialist skills within your organization.

Level 2

Readiness and Process Advantage

You have formalized company standards, practices, procedures and skills that give you an advantage for execution. You have partially documented your approach and priorities, and acquired some specialized skills within your organization.

Level 3

Execution Advantage

You're exploiting advantages with mature processes that capture outcomes. You're measuring trust and regularly checking your approach with customers to drive continuous improvement. Last, but not least, you have complete documentation of your approach, including roadmaps for implementation, and a complete set of appropriate skills to support the implementation of trust within your organization.

Case Study

While each company's trust journey will be individual, the principles and maturity levels are designed to be generally applicable. To help illustrate how the principles can be used to chart a path toward increased trust, we will consider how a fictional start-up — PersonConnect — could progress to higher maturity levels in each area.

HR and recruiting are important areas for artificial intelligence (AI) investment, both because they are cost centers that benefit from efficiency improvements, and because hiring and empowering the right people is so critical to business success. AI promises to make things more efficient through process automation, and also to provide valuable insights, freeing HR teams from low-level tasks and helping them to operate in a strategic and data-driven way, and to build high-performing teams.

PersonConnect is an AI-enabled applicant tracking system and HR information system. Its chatbot engages prospective candidates and gathers information for their application, walks new hires through the onboarding process, and allows employees to ask questions about HR topics. HR teams can use the system to gather data on employee engagement and performance and hiring efficiency, and to automate standard HR processes.

Because HR data can be highly sensitive as well as highly valuable, the leadership team at PersonConnect wants to differentiate on trust. While the company has to date focused on building out the core functionality to compete with established players, it is now seeking to become the most trusted name in its space. Employees are excited about the new direction and have started to gather customer requirements, but the company has little established process and no plan for how to share its new focus with customers.

We will take PersonConnect through our trust framework and show how each principle contributes to a comprehensive trust strategy.

PRINCIPLE 1:

Create new value through trust.

Look for opportunities to create new business value through trust.

Level 1

You have spoken to and understand how to build trust with your customers.

Level 2

You have built trust with existing customers.

Level 3

You create new value through leveraging your trust with customers.

Building trust with your customers goes beyond compliance; it is about creating new value for customers and for the company. For example, building trust can lead to increased willingness for customers to share data with you, which in turn can be used to create new business value by training machine learning algorithms.

To prioritize opportunities to build trust, talk to your customers to understand the value they derive from your product and their degree of comfort with your solutions, practices and brand. Map your customers on the Value/Comfort Matrix on page 3 to help identify those that are both at risk of churn (due to low perceived value or comfort) and strategic to the business. Next, take the necessary steps — whether by increasing the value you deliver or a factor of comfort — to reach trust. This will become your trust roadmap.

To increase value, you may need to build additional functionality. If functionality exists, but customers are not realizing value, you may need to address product reliability or reconfigure onboarding for these features to validate business outcomes and ROI cases.

How you build comfort with your customers will depend on your industry and the products that you offer. For instance, if you handle sensitive data, such as in healthcare and financial services, privacy and security may be top of mind for your users. If you are using AI to make high-stakes decisions, such as in fraud detection or recruitment screening, fairness and explainability may be major concerns.

Each incremental increase in the value you provide may require you to increase comfort to drive adoption. Conversely, increasing comfort can itself drive more value. For example, making systems more transparent with explanations can also improve customer satisfaction and increase product adoption. Keep in mind that situations that may seem like trade-offs don't always need to be. Take advantage of win-win opportunities where you can enhance value and comfort at the same time (see Find Win-win Opportunities on page 12).

Be strategic in your investments and beware that excessive focus may start to yield diminishing returns. For example, addressing all potential security threats is impossible and could occupy valuable resources that would be better dedicated to more pressing threats to trust. The best companies find harmony between driving value, providing comfort, and efficiently using their limited resources.

Action Items

Conduct customer interviews with your success team to gauge where you stand on trust with your existing customers. Identify gaps and work to bridge them to build trust through improvements to the value and comfort you provide.

Be strategic in your investments in trust. Look for win-win opportunities and beware of diminishing returns.

Leverage your foundation of trust to access additional data and build incremental value over time.

Assess your customers' knowledge of AI trust issues and help to educate them on the gaps.

PersonConnect balances high data sensitivity with utility.

Since PersonConnect has undertaken a customer review to see where it can improve trust with customers, it has achieved Maturity Level 1 and is putting a plan into place to move to Level 2 by bridging the gaps to trust with its most important clients.

Because of the highly sensitive nature of personnel data, PersonConnect understands that trust can be a differentiator for the company. The leadership team wants to leverage machine learning in their roadmap to build explainability into the product, but early results indicate that to create a truly valuable product, they would need to create a cross-customer dataset. The team believes that customers would not grant expanded rights to their data until they increase the comfort in their product.

To validate their intuitions, they decide to talk to all of their customers about the value they derive from their products and the comfort that they feel with the company's data and governance practices. The team uses the results to identify the most common gaps to trust among PersonConnect's customer base. The results of the customer research are discussed internally and form the basis of PersonConnect's trust roadmap. Through the remainder of this case study, you will see the decisions that PersonConnect made to build trust with its customers.

Find Win-win Opportunities

The best companies move beyond a trade-off mentality and take advantage of new technologies that can bolster value and comfort at the same time. Here are some examples:

- Differential privacy is a mathematical calculation of how effective a particular privacy technique — such as injecting random noise into a dataset — is at protecting the privacy of individuals within that dataset. It improves performance and provides measurable privacy guarantees.

  Read our CEO's Guide to Differential Privacy to learn more about how differential privacy can help your company improve your machine learning models.

  - **value:** Performance
  - **comfort:** Measurable privacy

- Decentralized machine learning methods such as federated learning help companies ensure privacy through on-device modeling while reducing the cost of collecting, storing and protecting sensitive customer data and using significant compute resources to train aggregate models.

  - **value:** Personalization
  - **comfort:** Privacy

- Authentication solutions such as thumbprint access can improve security as well as usability, since users no longer need to keep track of passwords.

  - **value:** Usability
  - **comfort:** Security

DESIGN

PRINCIPLE 2:

Build trust into your culture.

Operationalize trust through data values and organizational governance.

Level 1

Your intent to build a trust culture is strong, but low on specifics.

Level 2

You have specific values supported by training.

Level 3

Your data values have become core to everyday operations.

Implementing trust in your organization requires that everyone understands the responsibilities that come along with access to customer data, starting with the CEO. To achieve this, unify and clarify your approach by writing your data values to explain how you think about and handle data (see sample data values on page 15).

Data values constitute a public commitment to customers and partners on how you will care for their data and respond in a time of need. When developing your own data values, align them with the sensitivity of the data being collected.

Without structures and processes to support proper data management, you leave your employees exposed to judgment calls. Instead, be clear on the expectations when handling sensitive data. Build a culture of trust where employees seek to do the right thing and feel comfortable questioning and challenging the status quo. Acknowledge and recognize employees who demonstrate success in the areas of trust.

Messages on trust should consistently and frequently come from the top — the CEO, C(I)SO or Chief Trust Officer. This makes it clear that trust is an organizational priority.

The extent to which senior leadership supports the objective of becoming a trusted company will directly impact your success.

New hires in all roles, from entry level to the C-suite, should be evaluated on not just their abilities, but also how much you can trust them with your organization's and customers' sensitive information.

Avoid delegating responsibility for trust across many individuals or teams. Problems arise when trust becomes a compliance or checklist item that is constantly traded off against other product priorities with no organization-wide coordination or authority.

The best companies will appoint a senior executive responsible for trust delivery. Where possible, they should report directly to the CEO. Even companies that have adopted the right way of thinking will still run up against conflicting interests. To be successful, the trust leader needs to have significant influence within the company. Ideally, the Chief Trust Officer (or equivalent) will also be an officer of the company and participate in leadership, marketing and product decisions.

Action Items

Make trust everyone's responsibility, and include an assessment in performance evaluations to underline its importance.

Discuss trust openly, addressing both positive and negative examples. Encourage open discussion and ideas.

Appoint a trust leader who reports to the CEO. Make it their primary responsibility to build a culture around trust.

Implement ongoing employee testing to ensure consistent compliance with security practices.

PersonConnect integrates trust into organizational planning and process.

Because the PersonConnect leadership team already has a strong commitment to developing trust as a core value, they have achieved Level 1 and are looking to move to Level 2 by formalizing values, leadership and training.

While the PersonConnect team isn't able to add a senior-level executive this year for budgetary reasons, they hope to hire a Chief Trust Officer after raising their next round of capital. In the near term, the CEO is serving as interim Chief Trust Officer and has convened a cross-functional trust team to map out accountability across the organization and ensure the whole company participates in developing the company's trust roadmap.

The team's first task is to develop a set of data values. The team looks at standout companies for inspiration, and is holding interviews with employees and customers to help hone their values. The company is hoping to share them publicly next quarter.

Even while data values are being refined, the CEO has tasked the HR team with integrating the first draft of them into all personnel processes. Questions about trust are part of all interviews and have been integrated into performance reviews. New employees are trained on trust as a part of onboarding, and the company aims to hold team-specific training for all existing employees over the next few months. Each training session will be introduced by the CEO to emphasize that trust is a priority.

Share Your Data Values

Data values can vary significantly from company to company. Here are a few strong examples to inspire yours:

Data attribution and ownership — "Your data is yours."

Data integrity — We respect original data and indicate when and how it is modified for the purposes of data standardization and enrichment.

Data purpose — We use your data for the agreed purpose and no other.

Product function and data privacy — We strive to improve our products while maintaining your privacy.

Control — We make it easy for you to decide what functionality you value, how you would like your data to be used, and when it should be deleted.

Fairness — We proactively identify potential sources of bias in the data before it is used in any downstream process such as model training.

Data retention — We do not retain your data any longer than needed for the purposes directly agreed with you.

Data sharing — We never share your data with anyone outside the organization without your explicit permission.

SECURITY

PRINCIPLE 3:

Design resilient systems to reduce the impact of an attack.

Assume that you will get hacked.

Level 1

Some knowledge and implementation of security principles exist in your organization.

Level 2

Security principles are incorporated into your application architecture.

Level 3

Your data values have become core to everyday operations.

No system is impenetrable. The larger, more complex, and more visible the system gets, the more likely it is to eventually get breached. Three approaches that have been shown to minimize the impact of compromise are the principle of least authority, decentralization and redundancy.

The principle of least authority states that systems should never grant access to more resources than are required to complete the task. This is true for software, but also for human-based systems such as granting physical access to an office building after hours. Organizations should ask themselves whether the access is really required. If not, don't provide that access, or limit it to certain times or certain physical areas.

Decentralization applies to both human processes as well as software architectures. When two individuals are required to approve a financial process or to add a user to a software system, a human process is decentralized. An example of decentralization in software architectures is found in bitcoin and blockchain, where the public ledger that tracks all transactions is distributed across thousands of nodes. For the integrity of the ledger to be compromised, 51 percent of those nodes would need to be controlled by a single entity, which becomes increasingly unlikely as the number of nodes increases. Decentralization can also be achieved with a micro-service architecture and structured design, which, in contrast to a monolithic system, can deliver security advantages by limiting access to data and other system resources.

Finally, redundancy helps to address increasingly common Denial of Service attacks, including attacks often executed by large-scale botnets. For example, top-tier cloud providers such as Amazon Web Services, Microsoft Azure and Google Cloud all provide logically and geographically redundant services, protecting against cyberattacks, physical breaches, and even natural disasters.

Action Items

Assess your current security architecture — including any third-party products you've incorporated — to find areas of strength and potential vulnerabilities. If you don't have the expertise in-house, engage an outside security specialist.

Audit physical and software permissions regularly to ensure you are respecting the principle of least authority as needs and roles evolve.

Invest in top-tier third-party applications to take advantage of their security technologies.

PersonConnect focuses on the three principles that protect attacks from spreading.

Because knowledge of the three principles is limited to specific individuals within the organization, PersonConnect is currently at Level 1. The team wants to move to Level 2 by formally incorporating consideration of each principle into their product and processes.

On the customer end, PersonConnect already supports the principle of least authority — with different permission levels available for employees, team managers and HR personnel using the system. However, internally, PersonConnect customer success managers and developers have a single level of access that includes the ability to see and change all customer data. While access and all changes are logged and the logs are periodically audited for misuse, the team knows it must improve internal access to better respect the principle of least authority.

Decentralization presents a bigger challenge. Both customers and the support teams that serve them are concerned that there will be a drop in efficiency if two individuals are required for common operations such as changing employee data, or adding and deleting users. PersonConnect's product team has decided to investigate other products that have implemented decentralized workflows and then run tests on a few alternatives.

PersonConnect is already using AWS and feels it is meeting the industry standards for redundancy given its stage. However, the CEO is working on developing a more rigorous review process going forward to evaluate any relevant infrastructure changes.

PRINCIPLE 4:

Construct a rapid remediation plan and practice using it.

When a breach occurs, be prepared to respond quickly and effectively.

Level 1

Your remediation plan has limited scope and applicability.

Level 2

Your remediation plan is comprehensive and widely known.

Level 3

You proactively update and practice your remediation plan.

Many organizations have formal plans for disaster recovery, but unfortunately most do not have comprehensive remediation plans in case of data compromise. When an incident does occur, the plans are often ineffective because they haven't been tested and practiced ahead of time.

Investing in security will reduce the probability of needing to use the plans, but there will always be latent risks. Make it clear to customers and employees that you've taken reasonable steps to understand, manage and reduce these risks.

Effective plans cover both common scenarios and corner cases. They should include specific actions, quantifiable data, and steps to prevent similar incidents in the future. In the case of data compromise, plans will explain procedures for determining how data was affected and how the system may have suffered from being infiltrated.

When practicing the plan, be sure to involve all relevant stakeholders within the organization. The most effective drills don't happen at predictable times of day, when everyone is at work. Try to make things as realistic and high-energy as possible. Hold live meetings with key people, including the CEO, CTO, and any software developers dealing with the incident. Include other teams such as customer success, sales, marketing, human resources and legal, all of which would play a role in a real incident.

Consider emulating a real breach by hiring professional "white hat" hackers to attack a replicated test environment that mirrors production. The more realistic your practice sessions, the more likely you will succeed during a real attack.

Yahoo![2] and Target[3] are two examples that show how poor incident response directly affects the technical and PR damage of a major breach. In both cases, the companies had detailed incident response plans that proved to be poorly designed. Neither demonstrated a proactive response approach and, in the case of Target, it was reported that warnings were issued from its monitoring system and ignored before customer data was stolen.[4]

When incidents inevitably do happen, use the learnings to re-prioritize and accelerate your security

2 "Yahoo 'irresponsible' over data disclosure, says PR — or can it win public sympathy?" PR Week. September 23, 2016. Retrieved January 1, 2019.

3 "To Regain Trust, Target Must Do More, Crisis Experts Say." New York Times. January 10, 2014. Retrieved January 1, 2019.

4 "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." Bloomberg. March 17, 2014. Retrieved January 1, 2019.

roadmap. Examine what failed in the organization that could have stopped the attack. Look at technology and process gaps, failures in the threat model, security awareness across the team, and the amount of resources allocated to mitigating threats. If the threat was known to be unmitigated, evaluate whether the damage incurred is consistent with your original estimate for this particular threat.

While we often read about data breaches, we rarely hear about the steps that companies take to fix them and improve their infrastructure. In 2014, JP Morgan Chase suffered a major data breach impacting 76 million households and 7 million small businesses.

By 2016, the company doubled its cybersecurity spending to more than $500 million, investing heavily in new technologies to strengthen its network and detection capabilities. Today, JP Morgan is regarded as the gold standard in both banking and cybersecurity, with more assets under management than any other North American bank. Even so, company officials understand the target on their back, with CEO Jamie Dimon identifying cyberattacks as the "biggest vulnerability… for just about everybody."[5]

Action Items

Develop your company's remediation plan and threat model, or update your existing plan if you have one.

Plan your next simulated breach and set up a recurring schedule thereafter.

PersonConnect builds a remediation plan from scratch.

Since PersonConnect has no remediation plan yet, it has not yet achieved Level 1. Its focus is on rapidly building out a basic plan and then moving quickly to Level 2 by involving a broad range of stakeholders in its development.

The company has focused on building core functionality, including security features, and has not experienced a major breach to date. As a result, PersonConnect has not created a rapid remediation plan or detailed threat model. The trust team recognizes that this needs to change, as the company will become more vulnerable as it grows and becomes an industry leader.

To begin this process, the trust team analyzes several recent breaches in the news — both from within the industry and outside it — as well as how companies chose to respond. They develop hypothetical scenarios for PersonConnect and brainstorm ideal responses — including not only how to respond to the breach, but how to communicate about it to customers and the public. Additionally, the communication team proactively informs customers about how they currently protect their security.

Because the company has limited full-time resources to devote at this stage, the CEO decides to hire consultants in a few key areas: white hat hackers to test for vulnerabilities, and a crisis communications professional to engage in the event of a high-profile breach.

5 "Jamie Dimon says cyber warfare is the biggest risk to the financial system." CNBC. September 20, 2018. Retrieved December 27, 2018.

PRINCIPLE 5:

Understand customer and regulatory privacy requirements.

What you don't know can hurt you. Get ahead of privacy issues, and reduce exposure by identifying and mitigating risks.

Level 1

You reactively respond to privacy issues with a compliance lens.

Level 2

You proactively manage your data sources, considering both regulatory and customer requirements.

Level 3

You not only map the risk landscape, but shape it proactively.

The most effective way to reduce your privacy risk is to avoid unnecessary data collection. If collecting personal data is a must, put processes into place so that as you no longer need the data you delete it immediately.

Next, map out your data requirements and consider what might change the level of trust that has already been built with your customers. Extend your thinking to your partners and suppliers. Are there any transparency concerns around the origins of your third-party data? Conversely, could your practices be putting a downstream partner at risk?

With your data sources mapped, study the jurisdiction-specific privacy requirements and trends. This is especially critical if your business operates in multiple geographic areas, as different jurisdictions often have different requirements around privacy, data retention and lawful access — sometimes even in direct conflict with one another.

The privacy discussion never stays still — new privacy-preserving techniques are emerging, and new regulations are under debate. Customer perceptions and demands also continue to shift as privacy violations figure prominently in the news. The best companies will continually refresh their understanding and adopt new technologies and practices.

Action Items

Assess what personal data you need and what risks you create by collecting, storing, using and sharing it.

Map your data sources and their corresponding legal and regulatory obligations.

Seek out ways to expand privacy expertise in your company and provide your unique perspective to the industry.

PersonConnect looks outward to stay in the know.

PersonConnect currently is at Level 1, primarily focusing on privacy from solely a compliance standpoint. It is hoping to move toward Level 2 by deepening its understanding of legal requirements and expanding its requirements to incorporate customer needs and industry trends.

While international expansion is on PersonConnect's long-term roadmap, the company currently only serves clients in the United States. Because product functionality is designed in part to help customers comply with state-by-state HR laws, the legal team stays abreast of relevant laws where PersonConnect has current or prospective customers and keeps other teams in the loop. To date, however, they have focused less on privacy and data protection laws in their analyses.

PRIVACY

PRINCIPLE 6:

Give customers control and oversight over their data.

Show customers you care by providing user-friendly controls that are simple to understand.

Level 1

Customers can view or manage their data by going through a manual support process.

Level 2

Customers can view and manage their data easily.

Level 3

You not only provide users with data usage controls, but educate and encourage them to help them make the best choices.

Consumer software companies have traditionally established very broad data rights in order to future-proof the business, following the philosophy that more data is better. Users often have little to no understanding, visibility or control over how their data is collected, stored, used or shared. However, this approach is now incompatible with international legislation and increasingly, customer demands.

B2B software companies are typically at the opposite end of the spectrum when it comes to data rights. Most B2B companies have highly constrained contracts that limit or eliminate the possibility of cross-customer data aggregation and sometimes even prohibit using even an individual customer's data to improve the system or services.

The most successful companies are those that create products that protect customer privacy by default. They review each data type they collect and ensure that it has a purpose, communicating the purpose back to the customer. Users understand how providing their data returns value and can easily opt in or out anytime they choose.

Your company should drive the conversation around consent and acknowledge that data ownership remains with the customer. It's important to explain the value that you provide in exchange for access to each piece of data to inform your customers' choice. Software teams should incorporate privacy into the development process and provide tools that give users visibility into personal data and how it is captured and stored.

An open dialogue around privacy encourages users to think about their data more frequently. When appropriate, remind users that an action has a privacy implication and ask whether they want to review their settings. For example, iPhone apps ask users to enable access to camera, microphone or location services only when this functionality is required. Social media platforms send alerts to check whether users want posts to be public or whether they would like to adjust their privacy settings.

Make settings optional and granular to encourage engagement. As users learn to trust the system and understand how sharing their information provides value back to them, they naturally become incented to share more and higher-quality information in order to get even more value from the system.

Action Items

Have a conversation about consent with your users and explain why you need certain data to deliver results.

Implement privacy management solutions to help your customers review and control the data that you hold.

PersonConnect prioritizes each user group's needs for control over their data.

PersonConnect is currently at Level 2, since HR managers can manage and configure data access using their administration functions. It is seeking to move toward Level 3 by helping proactively guide users as they share information.

PersonConnect serves several groups: HR teams, managers, job candidates and individual contributor employees. In developing a trust roadmap, the team considers the needs of each of these groups to understand and control what data they are sharing.

With the increasing scrutiny of employer surveillance of employees, PersonConnect sees an opportunity to differentiate by protecting the privacy of individual contributors. If these employees feel comfortable with the data they are sharing, they are more likely to use the system instead of other channels, benefiting HR teams. The team decides to prominently display controls for individual pieces of data (for instance, a cell phone number is usually shared with the entire organization, while the emergency contact is limited to HR only, and individual interactions with the chatbot are held entirely private).

The PersonConnect product team has derived a lot of value from usage data — seeing the most frequent support topics and website actions helps prioritize their roadmap. However, there is a concern that some customers do not understand the scope of the data collected. They decide to allow users to opt out, but to provide a benefit for users that opt in: they will share that company's usage data in aggregate form with the HR team, allowing them to understand which parts of the system employees use most as well as trends on commonly asked questions.

PRINCIPLE 7:
Root out bias.

Avoid propagating bias within your business, product and processes.

Level 1
You are informed about bias and committed to reducing it.

Level 2
You have a robust set of anti-bias processes throughout the company.

Level 3
You have quantifiable anti-bias KPIs supported by real-time reporting and monitoring.

Discrimination in all forms is under increasing scrutiny. Human bias can creep into your organizational practices when employees act on biased views, often without ever realizing it.

Increasingly, algorithmic bias also presents a challenge for companies that leverage AI. Machine learning is often portrayed as an objective, fair and data-driven approach to decision-making. However, fairness and objectivity only exist if data and models are free of bias. If your machine learning model is trained on biased data sets, your product or service will perpetuate unfairness and discrimination.

You can address human bias at the individual, team and organizational level. First, uncover individual blind spots by putting employees through self-awareness training on how to recognize their potential for implicit bias. For example, Harvard has an implicit association test to help understand deep-seated attitudes and beliefs.[6]

When working in teams, diverse backgrounds and experiences draw different perspectives, which means that members will be more able and likely to uncover and challenge each other's biases.[7]

Address bias in your organizational processes by using objective data to decrease subjectivity in decision-making. For example, use data from psychometric assessments, job samples and a systematic multi-rater interview process to reduce bias in the hiring process.

To mitigate the effects of technological bias in your solution use both a top-down and bottom-up approach. When defining the problem being solved, think about how and why bias could come into play. Identify protected groups and determine how bias might impact each of them. Make sure fairness requirements are written into your design, with the explicit intention of testing for and eliminating the most impactful types of bias.

When collecting training data, be aware of biases in the data you are collecting or in the data collection and sampling methods themselves. Consider, for example, whether your model performs better for one micro-segment due to larger population samples. If so, consider collecting additional data for underrepresented segments, while being aware of the risks of access to sensitive user attributes. If you are relying on human annotators, define strategies for labeling data to minimize annotator bias, and design mechanisms to recognize bias in labels.

During model training, think about fairness as an optimization problem and test whether performance

6 Implicit Association Test. Harvard University. Accessed January 9, 2019.

7 Why Differences Make a Difference: A Field Study of Diversity, Conflict and Performance in Workgroups. Administrative Science Quarterly, 44(4), 741–763. Karen A. Jehn, Gregory B. Northcraft and Margaret A. Neale, 1999.

is optimized for underrepresented segments. Before deployment, consider using FairTest or other bias-detection algorithms to automatically identify unforeseen sources of bias. Finally, make sure you have an ongoing governance process that takes into account any changes to input data or model weights. You should also periodically check that your model complies with relevant fairness regulations.

Removing bias once you've detected it presents its own set of problems. Simply deleting sensitive attributes from a model does not solve the issue of fairness because there can be correlations between the remaining attributes and those sensitive attributes removed. It may also make it harder to representatively sample. Leverage existing academic research to achieve good representation in the data while simultaneously obfuscating any information about membership in the protected group.

Action Items

Train employees on implicit bias to allow them to recognize their own biases. Set up team-level and organizational processes to challenge assumptions with diverse perspectives and data.

Incorporate anti-bias measures in all stages of product development and set minimum performance requirements for each microsegment of the user population.

Use frameworks such as FairTest, FairML or IOFP to help detect bias in machine learning algorithms.

PersonConnect differentiates with a proactive anti-bias stance.

PersonConnect has an existing set of anti-bias practices and a strong commitment to stand against bias and has started to measure algorithmic bias, placing it at Level 2. The team wants to move toward Level 3 by designing anti-bias goals and measures into new features they are developing.

Because preventing bias, harassment and discrimination is so important for HR in general, t is vital for PersonConnect to have an impeccable reputation for fairness. The CEO hopes not just to avoid perpetuating bias in PersonConnect's models, but eventually to provide functionality that will help its customers detect bias in hiring or compensation, enabling them to operate more fairly.

One possible issue the team identifies for their product is that their chatbot will be better at responding to queries more commonly asked by white males, since so much of their training data is coming from that population. They identify several possible solutions to mitigate this imbalance, such as seeking to acquire more diverse companies as customers and offering incentives in the form of reduced pricing to help build more representative training data sets.

Since the chatbot also engages with job candidates, another key risk is that various populations might respond differently in a way that amplifies bias in the hiring process. The team decides to overhaul the chatbot's persona and language to be more inclusive and engage an external anti-bias consultant to help them do so. While the product doesn't yet use AI to directly assess resumes, the team is also keeping in mind that if it does, they will need to assemble training data that does not amplify pre-existing recruiter biases.

PRINCIPLE 8:

Develop a fair model for value exchange.

A fair business model is vital to establishing a foundation of trust.

Level 1

You are committed to developing a fair value exchange with your end users.

Level 2

You are implementing a fair value exchange in terms of value and comfort.

Level 3

You constantly reinforce a fair value exchange for your company and ecosystem.

Create business models that are quantitatively and qualitatively fair to set up long-term business partnerships with your customers. Think carefully about what you need from your customers (e.g., data) and what you will offer to your customers in exchange (e.g., insights).

The best companies design reciprocal value exchange into their solutions.

If you're not able to provide value immediately, stagger your data collection over time. As your relationship deepens and you collect more data, ensure that you provide more value in return. Simply put, if customers feel that they are not getting sufficient value from the product, any issues around comfort will be more acute.

Companies should also pay attention to the fair exchange of value with the community in which they operate, their employees (and contractors and suppliers) and with the environment. Consider the possibility of unintended consequences, and take responsibility for how your product and team respond. For example, would your solution or organizational policies behave fairly in extreme circumstances, and do you have a mechanism for ensuring human oversight?

Would you be willing to lower business returns in a crisis to preserve trust? In August 2018, Verizon was widely criticized[8] for throttling fire department data usage during California wildfires.

Companies might also want to consider if there are special risks in using your product that might apply to minority groups, different genders, different age groups, people with disabilities or others. For example, a model to predict the next CEO for a start-up developed by Mattermark predicted white males would be most likely to become CEO because the training data contained many more historical examples of this.[9]

How might a malicious, dishonest, biased or purely profit-driven actor use your product? Could it impact others negatively? What policies or processes do you need to have in place to protect your users?

Once you've established a fair business model, clearly communicate the costs and benefits so that users can make an informed choice. If there are risks to using your product that you are aware of, share this information with users.

8 https://arstechnica.com/tech-policy/2018/08/fire-dept-rejects-verizons-customer-support-mistake-excuse-for-throttling/

9 https://georgianpartners.com/episode-74-avoid-bias-machine-learning-models/

Action Items

Examine your business model to understand what each user group is providing and receiving in return.

Assess your operations to determine if you are treating workers, communities and suppliers fairly

Assess your products and processes to see how they would behave in testing circumstances (e.g., natural disasters, mass adoption, or adoption by new or unexpected user groups).

PersonConnect seeks to add value for managers.

Having done some legwork to understand customer perceptions of value, PersonConnect is currently at Level 2. It is beginning to move toward Level 3 by identifying issues important to maintaining a fair value exchange in future.

HR teams tell PersonConnect that they value the product, because it takes away rote queries and paperwork. This frees their VP HR customers to concentrate on more complex issues. Individual contributors and job candidates appreciate the system, because they can get answers to their questions immediately.

Through customer research, the team identifies one user group where the picture is less rosy. The team discovers that HR managers see PersonConnect unfavorably because they spend a lot of time inputting data into the system, but they cannot get the data they need for reports because the report builder is too rigid for their needs. The team discovers that many HR managers export data to Excel to build their reports. PersonConnect decides to create a series of most commonly used reports specifically for HR managers.

To further ensure a fair business model, PersonConnect's trust team also spends some time thinking through extreme scenarios that might happen when its product is used. As the product gains increasing functionality, will it begin to replace human HR workers altogether? What happens if employees pose extremely sensitive issues to the chatbot that it doesn't know how to handle, such as reporting ethical violations? The team has not come up with definitive answers to these difficult questions, but plans to regularly review them and discuss them with customers to show that they are aware of the issues. Their Head of Product also joins an industry working group that is laying out a vision for how AI-enabled HR products can help HR workers take on more strategic and consultative roles.

RELIABILITY

PRINCIPLE 9:

Make trust measurable.

Use metrics to track your objective performance and demonstrate reliability to users and employees.

Level 1

Trust metrics are limited and ad hoc.

Level 2

You regularly produce a comprehensive trust scorecard.

Level 3

Your trust scorecard updates in real time and is proactively shared with all stakeholders.

Make trust measurable by setting objectives for the value and comfort you deliver for each component of trust, from design to transparency.

As you develop measures of trust, take stock of the actions your company takes to promote trust. For instance, you might record the number of security issues investigated, number of customer interactions discussing trust, or employees trained in aspects of trust. Add a discussion on trust to meeting agendas, project plans and roadmap discussions and track the actions they produce. This shows that trust is part of the day-to-day business and will help as you assess problem areas: are you underinvested or are your processes broken?

It is also important to assess the organization's achievements in each area. You might track how accurately models performed or how quickly customer requests were fulfilled.

Organizations should also develop quantitative and qualitative measures of customer trust. Use case studies with ROI to quantitatively measure the value you provide.

Qualitative techniques and surveys show how your users perceive your trustworthiness — both the value they accrue and how comfortable they are using your service. Use the insights to improve internally and to learn how to talk to customers about trust.

No matter which metrics are important to your company, make sure they incentivize positive behavior and do not encourage unintended undesirable outcomes.

When evaluating technical performance, start with industry best practices and standards to guide you. For instance, in machine learning and AI, this means validating models and measuring and reporting on their performance using metrics such as precision, recall, F-score and AUC.[10] Where necessary, go beyond these standards and create or adopt new ones that help with the objective analysis of different aspects of the system and your business as a whole.

Once you are tracking these measures, the next step is to share them with relevant stakeholders to lead the conversation and show your accountability.

10 Precision is the fraction of correct instances among all instances predicted. Recall is the fraction of instances correctly predicted among all correct instances. F-score is the harmonic mean of precision and recall. AUC measures the trade-off of precision and recall for binary classification. These are some examples of metrics in ML; usually each task in ML has its own set of evaluation metrics.

Action Items

Measure your investment in trust, your results, and the value and comfort you deliver. Are all three of these areas in alignment, and, if not, how might those disparities be corrected?

Research your industry's standard measures and emerging technologies that help to quantify trust, such as bias detection and differential privacy. Which organizations are leading in this area, and what can you adopt from them?

PersonConnect lays the foundation for data-driven trust.

PersonConnect is working on moving from Level 1 to Level 2 by developing its first trust scorecard.

Since trust is a new focus area for PersonConnect, the team decides to focus on a few basic metrics first, moving toward Level 2. As they are still rolling out the new strategy to employees, the CEO decides that she first wants to track how many employees are trained on a clear and accessible trust strategy, with a goal of quickly getting to 100 percent. She also wants customer success teams to schedule and log trust-related conversations with customers, also aiming to hit 100 percent over the next quarter.

The trust team wants to measure whether these efforts change people's mindsets. They decide to report on the number of trust-related feature ideas employees and customers submit to the product team for consideration. By tracking these over time, they hope to increase innovation related to trust. They also add questions on the key aspects of trust to both employee engagement and customer satisfaction surveys.

These initial metrics serve a useful function in getting teams to rally around concrete trust-related goals, but the team would also like to move to more sophisticated measures in the future.

PRINCIPLE 10:
Anticipate the unexpected.

Things will go wrong. When they do, make sure you're well positioned to minimize the impact.

Level 1
You analyze and respond to failures.

Level 2
You proactively plan to contain fallout from failures.

Level 3
You detect and respond to failures quickly and efficiently.

Your reputation and the trust of your customers is built on reliable and consistent product performance. Even with the best of intentions, every company needs to be prepared for when things go wrong. It's not possible to predict the unexpected, but it is possible to prepare and build for business as usual in challenging circumstances.

How you anticipate, prevent and contain failures directly impacts your customers' trust. When incidents do occur, many organizations fail to address the root cause, because they can't get insights into what went wrong, or they don't have a clear escalation process from support to senior leadership.

If you track system performance metrics and set thresholds to identify abnormalities, it's easier to find and remedy the root cause to minimize the impact of failures. Continuous monitoring can help you see abnormal activity and investigate before things get out of control. You can also hire third parties to conduct penetration testing and audit the metrics you monitor.

The mindset of metric monitoring should be built into system design, so that when the metrics breach their threshold, systems automatically enter recovery mode and send alerts. This ensures that incidents do not get overlooked and deteriorate, unbeknownst to you.

Even still, you may have performance issues that are slipping through, but are noticed by your customers. Product usage data can reveal whether there is confusion around your workflows for you to improve. Setting up a social listening and customer feedback process will also allow you to track and respond to common issues.

It's hard to create processes during an emergency, so be clear on accountability ahead of time. Clarify each employee's role and function during recovery, and practice through drills. If there are rare and valuable skills on your team, ensure cross-training so that you have redundancy.

How you respond to adversity can buy you goodwill and build trust. When you face challenges, communicate openly and honestly about what has happened, who was affected and for how long, and what you have done in response.

Action Items

Anticipate failure from the initial design phase. Ask “what if” on possible system module failures to create contingency plans and practice them.

Define system health metrics, and establish a business success baseline so that situations can be monitored.

Invest in a team and tools to monitor, analyze and respond to unexpected situations.

PersonConnect prioritizes earlier detection for outages

PersonConnect is at Level 1, handling outages reactively, but is working to rapidly move through Levels 2 and 3 by implementing response plans and monitoring.

In working to quickly build functionality and scale up the user base, PersonConnect has failed to make reliability a key priority early on. All that changes when a catastrophic outage hits the product during a holiday weekend. When systems go down, job seekers communicating with the system are suddenly cut off. HR teams at customers hear from their employees that they cannot use the system, but they are unable to get a timely response from PersonConnect as to what is happening or when they can expect resolution.

Once PersonConnect becomes aware of the issue, it quickly convenes a team to restore the system. Fortunately, data has been backed up, but restoring it takes more than a day. The root cause is determined to be a local power outage caused by thunderstorms. PersonConnect’s on-premises server is identified as a single point of failure and the team begins investigating adding a redundant server in a different location or moving to a cloud architecture.

After this incident, the team conducts a post-mortem. While the underlying technical issues are solved, the CTO stresses the need to prepare for the unexpected going forward. The team decides to implement several measures to improve their response to future issues. First, they set up automated monitoring that will alert an on-call employee if either the number or length of conversations drops below a typical threshold. They also create a 24/7 hotline for customers to report emergency outages. The customer success team shares this action plan with customers as a first step in restoring trust.

TRANSPARENCY

PRINCIPLE 11:

Explain yourself.

Understand the explainability expectations of your buyers and users, and design your organization and its products accordingly.

Level 1	Level 2	Level 3
You're motivated to understand the explainability requirements of your users.	You address the top explainability pain points.	Explainability is used as a competitive advantage.

Organizations have an opportunity to build trust by focusing on making systems, business policies and procedures, and products more explainable. The first step should be to understand market expectations around explainability for both the buyer as well as product users, who may not be the same people.

Examples of what product buyers may want to see include information on your organization's cultural values and business ethics, supplier lists and any related selection criteria, hiring practices, and even documentation on internal processes such as how product features are prioritized.

For product users, an organization may have to provide information about why a particular recommendation has been made, an estimate of its impact, and even the ability to access an audit trail in high-impact automated decisions.

Develop an understanding of these groups including job roles, workflows, work environments, the lexicon they use, and any remaining pain points. Build your evidence by observing customers as they use the product and listen to sales calls to hear the needs of prospective customers. Once you adopt this mindset, apply it to your products as well as your organization using interpretable models that make it possible to provide explanations. For some users, technologies that allow for greater explainability and more interpretable results are essential. For example, radiologists using assistive technologies need to see which areas of the scan it used to make the decision. Similarly, some regulations impose explainability requirements; for instance, the GDPR requires fully autonomous systems to explain every decision they make.

In general, people prefer[11] short explanations — two or three bullets — that contrast the result against another. For example, for a credit score, you might provide two factors that would help to get a higher score, especially if one of them has disproportionately influenced the outcome. Or, for instance, you might show that you are basing a recommendation on data points of similar users.

Explainability should not come at the expense of model performance. Done well, both are possible. Those who have adopted explainability find several advantages. By better understanding the workings of the models yourself, you are able to generate and test hypotheses based on results, protect yourself from adversarial attacks, and monitor for bias.

11 Explanation in Artificial Intelligence: Insights from the Social Sciences. Tim Miller. August 15, 2018.

Action Items

Understand the explainability requirements from the perspective of the end user and relevant regulators. What are the hard requirements? What are the nice-to-haves? Work backwards to satisfy these requirements in product and process design.

Design systems and algorithms to have the right level of interpretability to support explanations, but do so in a way that also satisfies accuracy and performance requirements.

PersonConnect embraces explainability in its early recommendation features.

PersonConnect is at Level 1, with a solid commitment to explainability but little practical experience implementing it. It is seeking to move toward Level 2 by adopting explainable methods for new features.

While PersonConnect is not yet using machine learning models to suggest actions to management, it is in the long-term vision. For instance, PersonConnect could rank job candidates based on the application data it collects from them, or it could nudge managers to consider a raise or a promotion for certain employees that seem overdue. Because of this, the team is very interested in starting to gain experience with technologies that facilitate explainability.

They soon discover a near-term opportunity to do so. The product team notices that users have started asking where they can go for help with a certain topic, and see that it's technically possible to recommend organizational experts on certain topics based on information already in the system. While the models seem promising, testing shows that they are only around 80 percent accurate. To prevent employees from losing faith in the system, they decide to show the reasoning of the model, to help them see the logic for the recommendation. For instance, the system might indicate that it has made a suggestion based on their job title, their longevity at the company, or their skills listed in the employee directory.

Communicate Your Approach to Trust

To effectively build trust, communicate the value and risks of what you are doing to your customers and partners in a way that's easy for them to understand. How you design trust will determine how you communicate it to others. Your communications should address what you mean by trust, what your customers can expect from a partnership with you, and the specifics of your processes around trust.

Ethical and legal issues surround automation and AI, so be prepared to support your decisions with a comprehensive, clear and defensible approach. The questions that need to be answered are complex, and it will take time to reach a consensus, so revisit your thinking regularly and be prepared to discuss and adapt your stance.

When describing what you have done, avoid using broad generalizations or meaningless phrases such as military grade encryption, complete transparency or we take security seriously. Instead, use simple and factually accurate descriptions of your controls and processes.

Trust is hard to build and easy to lose. No matter how well you do, there's always a chance that things can go wrong. When they do, respond quickly and decisively using a crisis communications plan that builds trust instead of weakening it.

Conclusion

Building trust with your customers is a significant opportunity to create mutual value through more productive relationships. To get there, you will need to deepen your understanding of what drives your customers and the value are they hoping to derive from your products and services. This will allow you to assess how you can create that value, what data you would need and what the best approach would be. Once you see the path to value, you can explore what would make your customers comfortable sharing that data and using those products.

The first step for any company looking to build trust with their customers is to understand where they stand today. The principles of trust and the associated maturity model can help you with that understanding and show how you can reach maturity in future.

Transforming your business around trust will not happen without a coordinated approach. Take a proactive, strategic, user-centric attitude. Design your trust program as a single initiative to ensure that your efforts around security, privacy, fairness, reliability and transparency are all focused on the same objectives. Finally, celebrate your approach to trust and share your successes and your struggles. An honest appraisal will help your customers to understand and appreciate your efforts.

Maturity Levels by Principle

Principle	Level 1	Level 2	Level 3
1. Create new value through trust.	*You have spoken to and understand how to build trust with your customers.* You conduct customer interviews to identify where you stand on trust with existing customers.	*You have built trust with existing customers.* You make the investments necessary to build trust with your customers.	*You create new value through leveraging your trust with customers.* You use trust-based relationships to access new datasets to create new value through trust.
2. Build trust into your culture.	*Your intent to build a trust culture is strong, but low on specifics.* Your leadership team sees that trust can be a core value of the company, but more specific data values are not codified and training is ad hoc.	*You have specific values supported by training.* A Chief Trust Officer owns the maintenance of corporate data values. Trust training is formalized and is mandatory for all staff, but infrequent.	*Your data values have become core to everyday operations.* Trust underpins company culture. Data values are understood and acted on by all employees, supported by regular training sessions.
3. Design resilient systems to reduce the impact of an attack.	*Some knowledge and implementation of security principles exist in your organization.* Some of your employees are familiar with decentralization, the principle of least authority and redundancy and consider them in application and process design.	*Security principles are incorporated into your application architecture.* The security principles are formally documented in design documents and you have started to implement them.	*Security principles are fully incorporated into all processes and technology and are a key component of the company culture.* You have a formal and detailed process that ensures that all processes and technology are incorporating the principle of least authority, decentralization and redundancy company-wide. Your teams are engaged in additional thought leadership to develop new ways of building system resilience.

Principle	Level 1	Level 2	Level 3
4. Construct a rapid remediation plan and practice using it.	*Your remediation plan has limited scope and applicability.* A remediation plan is in place for some threats, including a generic communications strategy. Leadership is aware of the plan, but no one else knows what to do in case of an incident.	*Your remediation plan is comprehensive and widely known.* A remediation plan has been evaluated and approved by a wide range of stakeholders in the company and covers most of the threats. The plan is practiced infrequently.	*You proactively update and practice your remediation plan.* A remediation plan is continuously updated based on data-driven analyses to cover all types of threats and is practiced regularly by all relevant parts of the organization.
5. Understand customer and regulatory privacy requirements.	*You reactively respond to privacy issues with a compliance lens.* You abide by privacy-related regulations for the jurisdictions in which you operate, but privacy is not core to your business.	*You proactively manage your data sources, considering both regulatory and customer requirements.* You have a thorough understanding of jurisdiction-specific requirements, customer needs and key privacy trends and use them to inform product development and data collection and use.	*You not only map the risk landscape, but shape it proactively.* Your risk landscape is updated in real time whenever data collection or jurisdictional needs change. You proactively identify and mitigate privacy-related risks through thought leadership, dialogue with regulators and adoption of privacy-preserving technologies.
6. Give customers control and oversight over their data.	*Customers can view or manage their data by going through a manual support process.* You are compliant with all relevant regulations and provide customers with their information or delete their data when requested, but there is significant effort required.	*Customers can view and manage their data easily.* You provide simple self-service controls and data usage information so that customers can manage access to their own data.	*You not only provide users with data usage controls, but educate and encourage them to help them make the best choices.* You build transparent interfaces to give customers control over their data. You proactively inform and guide the user through the data management process.

Principle	Level 1	Level 2	Level 3
7. Root out bias	*You are informed about bias and committed to reducing it.* Your employees in key departments such as HR, recruiting, data science and product are aware of potential sources of bias and make corrections on an ad hoc basis.	*You have a robust set of anti-bias processes throughout the company.* Employees receive training on bias and how to respond, and you are leveraging leading frameworks to measure algorithmic bias in your machine learning efforts.	*You have quantifiable anti-bias KPIs supported by real-time reporting and monitoring.* You have implemented goals, thresholds and processes for all employees to continuously monitor, seek out and rapidly respond to bias in processes, product design or algorithms.
8. Develop a fair model for value exchange.	*You are committed to developing a fair value exchange with your end users.* Your team understands the importance of developing a fair business model and understands some of the relevant issues, but does not have a comprehensive view of customer perceptions.	*You are implementing a fair value exchange in terms of value and comfort.* You have a plan and strategy in place to develop a fair business model. You prioritize features in your product that generate value for your customers.	*You constantly reinforce a fair value exchange for your company and ecosystem.* You have developed and executed on a fair value exchange with your customers, and also have a broader plan in place to think through the future impact of your business model.
9. Make trust measurable.	*Trust metrics are limited and ad hoc.* Individual teams collect and track some trust-related metrics, but without company-wide coordination or visibility.	*You regularly produce a comprehensive trust scorecard.* You measure efforts, results and user perceptions in all areas of trust, reviewing performance and setting goals on a regular cadence.	*Your trust scorecard updates in real time and is proactively shared with all stakeholders.* Comprehensive performance metrics are available in real time, and key metrics are communicated to customers and the public. You lead the development of new trust metrics to define best practices for your industry.

Principle	Level 1	Level 2	Level 3
10. Anticipate the unexpected.	*You analyze and respond to failures.* You conduct post-mortems when failures occur and fix underlying issues, but do not have a systematic way of catching or responding to outages.	*You proactively plan to contain fallout from failures.* You have an escalation, response and communication plan for common system failures and use it.	*You detect and respond to failures quickly and efficiently.* You monitor product and system health metrics and customer feedback channels in real time, and regularly practice and refine your response plan.
11. Explain yourself.	*You're motivated to understand the explainability requirements of your users.* You are aware of the benefits of greater transparency for your organization and your product.	*You address the top explainability pain points.* You've identified where opaque models and processes can hurt your customer experience the most and made the shift to more transparent methods.	*Explainability is used as a competitive advantage.* Product design, processes, and people all use transparency to engage employees and customers and get input for further improvement.

info@georgianpartners.com // georgianpartners.com

About Georgian Partners

Georgian Partners is a thesis-driven growth equity firm that invests in SaaS-based business software companies. We look for companies that use foundational technology trends such as applied artificial intelligence, conversational business and security first to dominate their markets.

Founded by successful entrepreneurs and technology executives, at Georgian Partners we leverage our deep software expertise to directly impact the success of our portfolio companies. That expertise spans areas as diverse as machine learning, analytics, deep learning, cryptography, linguistics, natural language processing, differential privacy, software engineering, information security and cloud computing.