15 STRATEGIC STEPS COMPANIES SHOULD TAKE TO SECURE CUSTOMER DATA

May 13, 2022 • Forbes

Collecting customer data can help companies improve their products and services. However, these days customers are increasingly wary about trusting businesses with their personal data. Stories of hacks of high-profile companies and growing awareness of the fact that some companies traffic their data for a profit have made many consumers think twice about sharing their personal information.

It's essential for companies to earn consumers' trust by committing to robust, comprehensive data security policies and sharing those policies publicly. Below, 15 members of Forbes Technology Council discuss steps every company that collects consumer data should take to protect it and how they can promote their data security protocols to help customers feel more secure.

Photos of featured Forbes Technology Council members. Members of Forbes Technology Council discuss strategic steps companies should take to secure customer data.

1. Carefully Negotiate Security Provisions With Vendors
Outsourcing business functions increases a company's financial and reputational risks from a breach. The customer and service provider often address these risks contractually. When negotiating security provisions in your contracts, consider the sensitivity of the information, the results of your due diligence in reviewing the service provider's capabilities and both parties' internal policies and procedures.
- Olga V. Mack, Parley Pro

2. Center Candidate Screenings On Data Transparency And Trust
Building trust must be a top consideration anytime sensitive data is in play. This is especially true in hiring given the massive talent shortage we're facing. For example, although background screening is important—especially for industries such as banking and healthcare—a candidate experience that centers on transparency and trust with sensitive data can be pivotal for securing the right hire.
- Andrew McLeod, Certn

3. Create An Organizational Function Focused On Tech Ethics
The first step is to make tech ethics a core organizational function. This new function will create policies, build a culture and install tools and processes. Tech ethics is a vast and complex issue that can vary greatly globally and from region to region. Until we, as leaders, operationalize how we collect and handle consumer data with care, we will not deliver a quality promise to our consumers.
- Ning Gao, Mayo Clinic

4. Leverage Ethical Hacking Services
Audits and compliance force companies to implement best practices in the technology stack. The problem is that often

companies have code issues that audits do not catch. Using ethical hacking services enables bugs that your team would otherwise miss to be found and fixed. We have seen massive success in our bug bounty programs.
- Jonah Kowall, Logz.io

5. Adopt Security By Design
Security by design, coupled with transparency, will take you a long way in your journey. Security by design involves several different areas, including educating employees, minimizing the amount of data that's collected, encrypting the data, carefully designing systems and managing who has access to them, focusing on security during the software development life cycle, and more.
- Rudy Shoushany, DxTalks

6. Only Use Customers' Data To Provide Value For Them
Each company that collects customer data should be honest about what they are trying to achieve and use collected data to provide value to customers, society and the nation, rather than just focusing on the commercial aspect. An organization's data center of excellence should develop good use cases, be on top of rapidly changing technologies and regulations and closely connect with the communications team to make messaging easy to decipher.
- Deepak Garg, Smart Energy Water

7. Ensure Comprehensive Compliance With Security And Privacy Frameworks
Get compliant with information security or privacy compliance frameworks required for the type of data you collect, store or transmit. That process will ensure secure data stores, the fail-safe transmission of data and the correct gathering of data. Additionally, vet any vendors that touch consumer data; third parties need to be compliant with infosec regulations or standards as well.
- Eva Pittas, Laika

8. Follow GDPR Standards (No Matter Where You Operate)
The EU's General Data Protection Regulation supports robust data protection. Sensitive information can only be shared with "explicit consent," and under the law, this must be communicated to consumers, creating a direct connection between the two parties. Running your services with a cloud infrastructure that's GDPR-compliant will boost consumer trust, no matter where your business operates.
- Tamas Kadar, SEON

9. Commit To Informed Consent
Informed consent can be the primary building block of consumer trust. "Informed consent" means that a company explicitly communicates to its customers what their personal data will be used for both now and potentially in the future, as well as how long personal data will be retained before the company must reobtain the customer's consent. Giving individual consumers the option to choose the length of time their consent is in effect could make the policy more personal.
- Amandeep Midha, Traive Finance

10. Regularly Remind Customers What Data You Have, And Let Them Opt Out
Tell consumers clearly and often what data you have and how you're using it, and ask if they would like to opt out. We do a quarterly health check with our consumers. We get so many notes back thanking us for taking the time and care to remind them that we are connected with them and that we respect their decision to opt out at any time.
- Meagan Bowman, STOPWATCH

11. Encrypt Sensitive Data
At a bare minimum, keep sensitive data in encrypted form. It sounds very basic, but surprisingly, a lot of companies overlook it—including

big ones like Twitter (it was a bug; but still). To make customers feel more secure, first tell them why you need the info you're asking for. Also, tell them that all consumer data is encrypted—not even company employees can read it.
- Vikram Joshi, pulsd

12. Have Processes To Accommodate 'Right To Be Forgotten' Requests

To secure and maintain customer trust, companies must ensure they're compliant with industry-standard privacy regulations such as GDPR, the California Consumer Privacy Act and HIPAA. Additionally, as a best practice, companies should have processes in place to accommodate "right to be forgotten" data requests—smart companies use automation to execute such requests at scale.
- Rich Waldron, Tray.io

13. Hire A Third-Party Service To Collect And Manage Data

If you are a small and unknown company collecting consumer data, I would recommend using a third-party service to do that on your behalf. For example, use MailChimp or SendGrid to store and process emails, use Shopify for e-commerce, and so on. Lots of software as a service products offer such services. Customers are more likely to trust their data to SaaS products than new companies.
- Arturs Kruze, Magebit

14. Keep At Least Three Copies Of Data

Businesses are custodians of any customer data they collect, and it is their responsibility to ensure it is stored compliantly and fully protected. We advise that companies keep at least three copies of data, stored on at least two different forms of media, with one offsite and one offline. Inform new and existing customers of any changes so they are comfortable trusting their data with you.
- Danny Allan, Veeam Software

15. Minimize Access To Customer Data

If data has to be collected, restrict access to only those who absolutely need access. Data should also have a known retention period, meaning once it's met usage requirements and is no longer needed, it should be deleted. Data for legal transactions should be archived securely. Such actions will help assure consumers that your company is protecting their data.
- Kevin Beasley, VAI