Insights, News & Events

10 WAYS GIG ECONOMY COMPANIES CAN PROTECT SENSITIVE CUSTOMER AND WORKER DATA

Insights
Nov 17, 2022

A recent blog post by the leader of a cybersecurity platform provides a suggestion as to how gig economy companies can protect all the sensitive data they accumulate – and we can add a few more items to that checklist. Arti Raman, CEO of Titaniam, provided a recommended approach she suggests to keep you protected when it comes to all of the personal information you collect from customers and workers. We have supplemented that suggestion with additional recommendations to offer a 10-step plan.

Importance of Data Security in the Gig Economy

Raman's October 28 post discusses how the gig economy has created a financial opportunity for millions of users, with an estimated 78 million American workers set to earn a projected $298 billion in wages by next year. Not to mention the tens of millions of beneficiaries of these services – either businesses relying on gig help or the end users directly receiving some benefit from the work.

But as Raman points out, this explosive growth is creating significant data risks. "Both gig workers and consumers share sensitive data with apps, ranging from freelance job sites to temporary lodging, ride-sharing, food delivery, and more," she notes. The information shared between parties includes user demographics, account information, financial data, social media updates, location tracking, and more. That makes gig economy companies a "target-rich environment" for cyber attackers.

What Can You Do About It? A 10-Step Plan

Related People

Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Richard R. Meneghello

Chief Content Officer

503.205.8044

Raman has one main suggestion that your company should take into account in order to protect this information. Besides this first idea, the Fisher Phillips Privacy and Cyber team has nine additional suggestions.

1. Raman suggests you deploy **full-featured processing on encrypted data** using a high-functioning data security platform. This would mean there's no need to decrypt data to provide highly performant search and analytics. "As a result, if cyber attackers penetrate networks, they are unable to access unencrypted data, even if they have highly privileged credentials, such as administrator keys," she says. This will protect you from ransomware attacks and payments since data can't be exfiltrated in clear.

2. Require **multifactor authentication** to access your internal network;

3. Keep **security software up to date** and institute timely patching of systems;

4. Enable **robust spam filters**;

5. Enforce **strong, unique passwords** with multiple characters (including numbers, letters, and symbols) and require that they be routinely changed;

6. Implement **robust cybersecurity user awareness and training programs** for new workers upon hire and at least annually for existing employees;

7. Immediately **disable credentials upon employee departure**;

8. Create **data backups** with regularity;

9. Ensure you have a **strong cybersecurity team** in place to not only monitor your network for vulnerabilities and any suspicious activity but also to develop and deploy an incident response plan (which should include response and notification procedures) in the event of a compromised system; and

10. **Develop an incident response plan ahead of time** so that you can immediately deploy effective resources if your business becomes the victim of a cybersecurity attack. An effective plan includes:

Service Focus

Privacy and Cyber

- Identification of key stakeholders and their responsibilities in the event of a security incident
- A plan for:
    1. Determining what systems were impacted and immediately isolating them;
    2. If affected devices cannot be removed from the network (or if the network cannot be temporarily shut down), securing the network by powering down infected devices to avoid any further spread of the ransomware infection;
- Triaging impacted systems for restoration and recovery;
- Retaining legal counsel to provide guidance in responding to the incident, including recommendations regarding potential data breach notification obligations and reporting requirements;
- Retaining a third-party incident response provider with experience in data breaches; and
- Reporting the incident to law enforcement.

Conclusion

Fisher Phillips will continue to monitor any further developments as they occur, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for mitigating the risk of those threats, please consult your Fisher Phillips attorney, the author of this Insight, or any member of Fisher Phillips' Privacy and Cyber Practice Group or Gig Economy Team.