Recent Data Breach at Twitch Exposes Danger for All Businesses

Insights
11.22.21

This fall has been a busy season for privacy professionals. From public education institutions and hospitals, to online broadcast and streaming platforms, we've seen a surge of data breaches that coincides with the upcoming holiday season – when cyberattacks are expected to rise even further. One of the more high-profile data breach incidents occurred in October when a trove of business-related digital information from a video game live-streaming platform was posted online for all the world to see. What can this incident teach your business about the need to ensure your compliance efforts are up to date?

Twitch Suffers Major Data Breach

Twitch – an online interactive streaming platform focusing on eSports & video games live streaming – suffered a data breach that was revealed to the public on October 6. Among the information hackers obtained and leaked were Twitch's source-code, internal security protocols, and earning records of many streamers. While no usernames or passwords were published, there's no guarantee that they were not compromised; only time will tell whether the breach also implicates such data.

Twitch became a huge target due to its status as a revolutionary interactive entertainment/streaming platform. It sets itself apart from traditional TV and other online streaming platforms by allowing the audience to interact directly with the host/streamer. The platform handles an estimated 9.2 million monthly users and provides lucrative earning opportunities for streamers and brands. With the sheer number of users' data, lucrative earnings, and industry notoriety, it's easy to see why Twitch was an attractive target.

However, businesses must remember that you don't have to be an edgy online-focused business to suffer a data breach. As long as you have customers or employees' data, then you are subject to the same risk. A series of compromised social security numbers or banking information, whether of customers or employees, can still be damaging when it falls into the wrong hands. Furthermore, businesses within the European Union (EU) jurisdictions or states with strict privacy regulations (such as California) may also face hefty administrative fines and costly civil litigation from such data breaches.

As we're now in the holiday season when frauds are on the rise, and with the continued popularity of telework presenting greater security risks, now is a good time for businesses to re-examine their

compliance obligations and data security protocols.

Understanding How Data Breaches May Occur

In order to prevent data breaches, businesses must understand ways that a breach may occur. Even if your business does not directly deal with retail consumers or is not an internet-based platform, the implications are all the same. Although not an exhaustive list, you should familiarize your organization with and address the following tactics:

- **Social Engineering Attacks**: A person may call, message, or email an employee and poses as a customer, employee, or an executive to manipulate the employee to reveal confidential information. For example, a caller may pose as an associate of a vendor and ask for the vendor's bank account number to confirm an order.
- **Phishing and Spear Phishing**: A cybercriminal may send an email claiming to be from a reputable entity (i.e., an established third-party vendor) or tailor an authentic-seeming message to a specific recipient, asking for confidential information (i.e. log-ins, bank account number, etc.).
- **Lack of Virtual Private Network (VPN)**: For businesses with employees working remotely, using an unsecured network at a public place, working on a shared device, or leaving their device unsecured in a public space present risks of data breach and unauthorized access. Implementing VPN and multi-factor authentication are some ways to establish a secured connection and prevent unauthorized access.

Data Privacy Regulations Implications

While a remote workforce presents more risks for a data breach, the privacy implications for failure to protect confidential and personal information are all the same – hefty fines and penalties – even if your business is non-internet-based or non-tech-focused. Businesses have a duty to protect employees and customers' confidential information such as social security numbers, drivers' license numbers, medical information, and financial account information, among other data. Now is the time for businesses to re-evaluate their compliance obligations and prepare ahead. Even if your business is not retail-centric, your obligations to employees' data alone can land your organization in hot water should a data breach occur.

For example, the General Data Protection Regulation (GDRP) applies if you process the personal data of and monitor EU-based employees, even if your business was incorporated or operates mainly outside the EU. Personal data is broadly defined as "any information relating to an identified or identifiable natural person." Such information may include an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of common identifiable personal information include address, date of birth, phone number, photos, email address, salary information, health records, and severance data. Other "special categories" of data such as racial or

ethnic origin, trade union membership, and biometric and health data (i.e., COVID-19 related information) may require enhanced protections.

On top of that, state-specific privacy regulations may impose additional (and complicated) compliance obligations for your business. For example, the California Consumer Privacy Protection Act (CCPA) applies to businesses operating in California that collect the personal information of one or more California resident and that satisfy one of the following thresholds: (1) generates annual revenue of $25 million or more; (2) collects the personal information of 50,000 or more California residents; or (3) derives 50% or more of its annual revenue from the selling of personal information. Even if your business doesn't meet any of the above criteria, but it is affiliated with or shares common branding with another business (such as a parent company) that meets the above, then the CCPA also derivatively applies to your business.

As you can see, both the GDRP and state-specific privacy regulations can be technical and complicated to comply with and follow. For this reason, you should begin your auditing and compliance processes early, and re-evaluate them on a regular basis, to allow room for adjustments down the road.

So There's a Breach – Now What?

In data security, prevention is an important duty, but not the only duty. Your response in cases of breach is just as important. Although not an exhaustive list, at the minimum, businesses should consider the following steps when dealing with data breach.

- **Contact Your Counsel and Cyber-Insurance Carrier**: Leave it to the professionals. Besides IT professionals, your legal counsel can help you analyze and comply with applicable data breach notification and other reporting obligations resulting from the breach. Furthermore, mitigating a data breach can be costly. As such, if you have cyber-insurance, you should notify your carrier in a timely fashion to maximize the likelihood of coverage for costs associated with remediating and responding to the breach.
- **Identify The Type of Information Affected and Initiate Your Incident Response Plan**: Mobilize your breach response team, and if you have an incident response plan, be sure to implement it promptly. Your protocols should include procedures to enable prompt investigation and remediation of the breach. Furthermore, you must determine the nature of the data at issue and how it was impacted by the breach to assess what legal requirements or regulations may apply. You may also want to consider whether to notify law enforcement.
- **Stop The Breach and Take It Offline**: It's already bad, don't let it get worse. Securing the network and changing network access authorization can be part of your response protocols should a breach occur. Whether it is to secure a physical area (i.e. where a computer was left unattended), to halt network access until further notice, or to take documents/equipment offline, you should put in place response protocols that are tailored to your business.

- **Contact Your Service Provider**: If a service provider is responsible for the breach (i.e. web security, website builder, 3rd-party payment processor), review any applicable agreements to determine the obligations of the parties and, as appropriate, ensure that the provider is investigating, remedying, and responding to the breach. You should also reassess their access privileges and verify that vulnerabilities were indeed remedied by the provider.

Conclusion

Unfortunately, the key question surrounding a data breach at your business is not a question of "if," but "when." As technology continues to evolve, there are an increasing number of ways for data breaches to occur. The bottom line is that regardless of the industry, you must always be prepared to adjust and revise your data security and privacy practices to stay ahead of legal obligations and defend against increasingly sophisticated cyberattacks.

If you have any questions about best practices for addressing data breach threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group. To ensure you stay up to speed with the latest developments, make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Service Focus

Privacy and Cyber