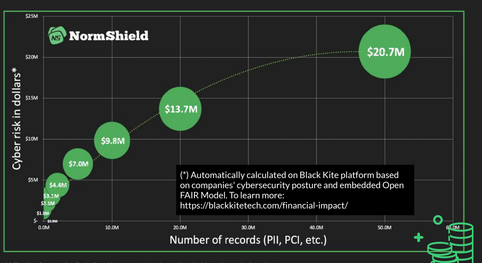
BLACK KITE

HOW MUCH COULD A DATA BREACH FROM ONLINE SHOPPING COST YOU?

As you count down the days until Santa arrives, cybercriminals are making their own checklist. Millions of online shoppers, e-commerce companies and their customers become targets of malicious actors every year, making data breaches inevitable. Hackers know e-commerce companies invest heavily in cybersecurity, therefore they're now finding a way in through third-party vendors.

To understand the real cost of a data breach, we look at cyber risk in dollars. Using the Open FAIR model, Black Kite calculates the potential impact (risk) to any organization in the case of a cyber breach.

In this report, we checked the cybersecurity posture of 10 online shopping sites in the U.S. from a hacker's view and computed the cyber risk in dollars. Depending on the amount of sensitive information kept, millions of dollars appear to be at stake.

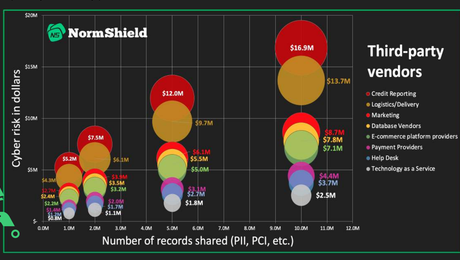


(‡) The list of companies (including third-party vendors) examined in this study can be found here.

The Cost of a Third-party Data Breach

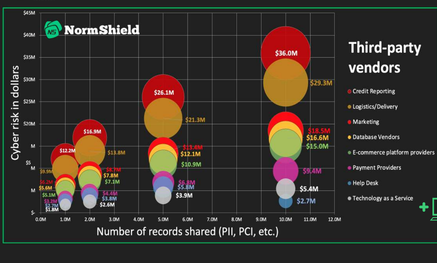
Data breaches caused by third parties increase each year as more companies share their data with third-party vendors. If the vendor's cybersecurity maturity is not sufficient, data breaches are highly probable.

Here, Black Kite analyzed some of the critical third-party vendors of e-commerce companies in terms of cyber risk in dollars. With an equal number of records shared with each third party, some vendors pose an even higher risk than the e-commerce companies themselves due to poor cybersecurity postures.



Internal Access Increases the Risk

Internal access to e-commerce companies will dramatically increase the cyber risk by almost threefold. In this case, threat actors may put their hands on more sensitive data.



Common Third-party Vendor Issues

Third-party vendors fail in three common categories as hackers seek to gain access to the data and personal information of e-commerce users and consumers.

Leaked Credentials

Hackers share usernames and passwords in combo-lists on the DarkWeb. Cybercriminals then use these lists to execute autonomous credential-stuffing attacks. With the right credentials, they can access sensitive data very easily.

Learn more about credential stuffing here.

Phishing Domains

Phishing domains targeting both customers and employees are threats for not only e-commerce sites but also their vendors. Many people receive e-mail scams impersonating third-party vendors such as PayPal or FedEx about their "recent order."

Do you know that phishing domains are increasing in the holiday season?

Expired SSLs

While online shopping, one of the important things to check is the padlock icon at the beginning of the URL. It is a sign of a secure connection certificate. The absence of such SSL/TLS certificates or their expiration shows certain vulnerabilities that hackers can exploit.

Learn six steps to harden your SLL/TLS strength here.

$$$$ At Stake Due to Third Parties

E-commerce companies work with hundreds of vendors, from delivery services to payment providers. A third party with a poor cybersecurity posture is a primary target for cybercriminals, especially in the holiday season. Any data shared with a third party may be exposed and cost millions of dollars.

Check out Security Current's Black Kite-sponsored CISO-authored report, CISOs Investigate: Third-Party Risk Management (TPRM) **here.**

REQUEST A FREE FAIR ANALYSIS REPORT ON YOUR COMPANY TO SEE THE PROBABLE FINANCIAL IMPACT ($$$) TO YOUR COMPANY, VENDORS, SUPPLIERS, OR TRADING PARTNERS.

GET A FREE FAIR REPORT

BLACK KITE