THE OSANO DATA PRIVACY AND DATA BREACH LINK

REVEALING A DIRECT RELATIONSHIP BETWEEN POOR PRIVACY PRACTICES AND DATA BREACHES

EXECUTIVE SUMMARY

Osano, the industry-leading data privacy platform, conducted a groundbreaking investigation into corporate data privacy practices.

Osano identified a direct relationship between organizations' privacy practices and their likelihood of experiencing a data breach.

During the research process, Osano's team invested more than 25,000 hours developing an innovative new rating scale for data privacy and then evaluating more than 11,000 websites.

The comprehensive study highlighted the following facts:

- Approximately 2.77% of companies reported a data breach over the past fifteen years.
- Companies with the least rigorous privacy practices are nearly twice as likely to suffer a data breach than companies with excellent data stewardship.
- The average company shares its data with 730 different vendors and third-party vendors. Third parties were responsible for two out of every three data breaches.
- Companies with the least rigorous privacy practices lose seven times the number of data records when they are breached.
- Hacker attacks were responsible for the highest number of data breaches and hacker-caused data breaches inflicted the most severe losses.
- Companies in financial industries were far more likely to experience data breaches caused by inside jobs.
- Nearly 30% of government and educational organizations with ".gov" and ".edu" top-level domains experienced a data breach.

After a thorough examination of the privacy practices from more than 11,000 companies and organizations, Osano identified three key trends for 2020:

- Increasing complexity of vendor policy changes and notifications
- Growing public concern about data privacy
- Expanding legislative activity addressing data security

INTRODUCTION AND CONTEXT

Launching an Idea

We've all experienced the uneasiness of clicking the "I accept" button before downloading an app or making an online transaction. Even if someone wanted to review the fine print of a website's terms and conditions, many businesses bury their privacy agreements in dense documents filled with legal jargon.

Our fears are well founded. We're constantly bombarded by news stories about data breaches that exposed people's personal information to the world.

From financial matters to social media, data privacy touches every aspect of our lives. But understanding what's really happening with our personal data requires fluency with legal contracts and expertise in digital security.

In 2018, Osano's founders searched for a system to determine the quality of organizations' privacy practices, as well as a simple way to know which companies shouldn't be trusted.

One problem: no such platforms existed.

So, they launched Osano — a B Corporation with a mission to protect companies, empower consumers, and increase transparency about data privacy.

Developing the Platform

The project started by building an extensive database of privacy documentation. Using Alexa Internet's rankings, researchers collected information from the top 11,000 most visited websites.

Osano assembled a team of two dozen attorneys to interpret and analyze the database of websites' privacy materials. These documents included Cookie Policies, GDPR statements, Terms and Conditions, and many other materials. To evaluate the scope of each policy notice, the attorneys considered 163 different factors, including (but not limited to) the following types of questions:

- Do they sell, share, or license data to third parties or affiliates?
- Do they use data for personalized, targeted, or behavioral advertising?

- Is any data about children under the age of 13 knowingly collected?

To make data privacy more accessible for the general public, the attorneys distilled that detailed qualitative information into one simple number — the Osano Privacy Score.

The Privacy Score rates each website on a scale from 300 and 850, similar to the scale used for personal credit scores.

Osano's team invested more than 25,000 hours assigning a Privacy Score to approximately 11,000 websites. Every night, Osano's software spider scans hundreds of thousands of pages. If a site changes its data policies or practices, the system records the new information. Substantial changes automatically prompt attorneys to reassess the website and recalculate its Privacy Score.

After spending all that time not only evaluating more than 11,000 websites but also developing an innovative new rating scale for data privacy, we gave the information away for free. Osano supports the vision for a transparent and trustworthy internet, so we established PrivacyMonitor.com as a free resource for people to find the Privacy Score for their favorite websites.

Forming a Theory About Data Breaches

During the process of developing the Privacy Score scale, a number of companies captured news headlines for major incidents related to data security. Upon closer inspection, many of the impacted companies had earned Privacy Scores in the lower rungs of the rating scale.

For instance, the Privacy Score identified Capital One's below-average practices several months before the financial company announced a massive data breach in July 2019.

This observation sparked a theory: perhaps there was a connection between a website's Privacy Score and its likelihood to experience a data breach. Osano hypothesized the existence of an inverse correlation: websites with high Privacy Scores were less likely to experience a breach and vice versa.

Confirming the Hypothesis

2.77% of websites reported a data breach over the past fifteen years

Osano investigated the theory that websites with insufficient policies were more likely to experience accidental disclosures, hacking attacks, and other data-related incidents. Profiles of data breaches from the past fifteen years were collected. **By comparing that information with the Osano datasets, the hypothesis was confirmed.**

The investigation continued several steps further, by analyzing additional factors, such as the number of records lost, the type of data breach, and the type of organization.

This report shares Osano's key findings about the relationship between data breaches and deficient privacy practices.

The vast majority of companies want to deal with privacy in a responsible manner. Prudent data policies can enhance customer trust and reduce financial liability. More importantly, companies can learn ways to protect their clients' information — without draining valuable time, attention, or resources.

MEASURING THE LINK BETWEEN DATA PRIVACY AND BREACHES

Categorizing Organizations by Privacy Scores

Data breaches are more common than most business leaders think.

Research indicates that approximately 2.77% of websites reported a data breach over the past fifteen years.

But not every business faces the same level of risk. Websites with inadequate data privacy practices are far more likely to run into problems.

Osano's analysis ranked websites according to their privacy practices and placed them into quartiles. Each quartile included a group of just under 3,000 organizations. Companies with the best Privacy Scores formed the top quartile and the companies with the lowest Privacy Scores composed the bottom quartile.

Top quartile:

- Average Privacy Score of 669.
- These organizations are making proactive efforts to be transparent about their data practices. Users can expect their policies to be readable and fair.

Second quartile:

- Average Privacy Score of 611.
- These organizations are generally good citizens of the internet. They may engage in some data sharing but usually with user opt-out consent.

Third quartile:

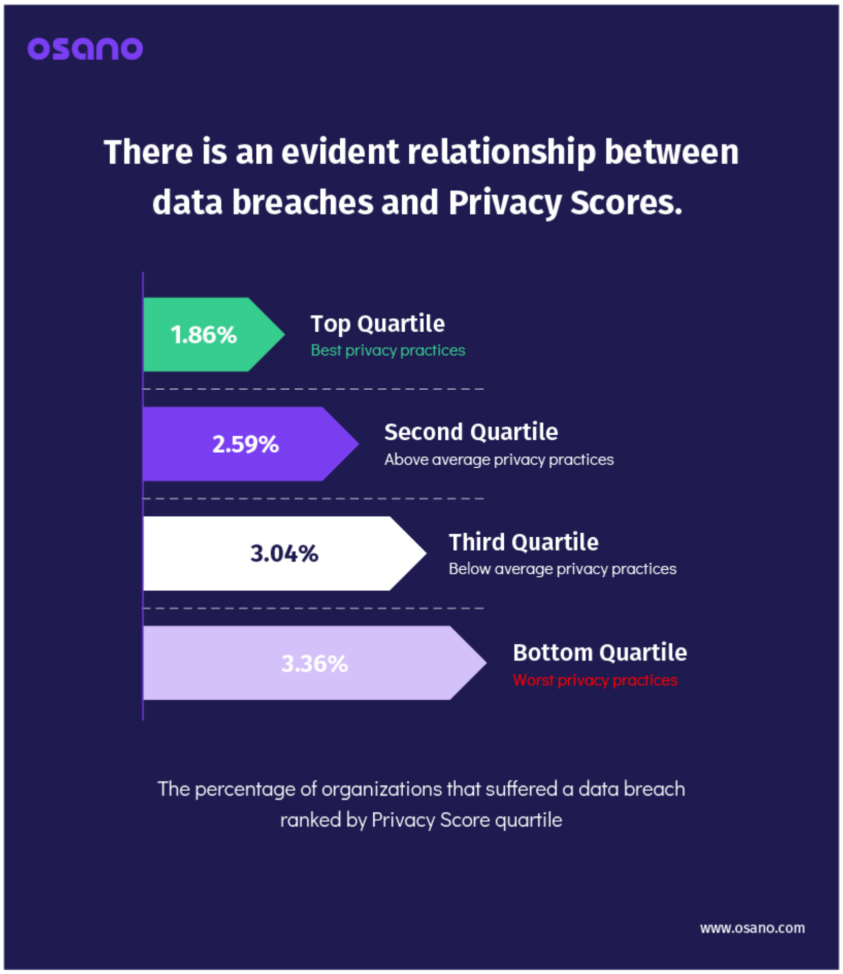
- Average Privacy Score of 563.
- These organizations may be sharing users' personal data without their consent, may be hiding onerous terms in their documents, and are likely to engage in data brokering.

Bottom quartile:

- Average Privacy Score of 493.
- These organizations may have extremely outdated privacy notices or no privacy notice at all. They may be known to engage in non-consensual sharing of sensitive data with third parties or are engaging in other data privacy practices that put users at risk.

Comparing Privacy Scores to Data Breaches

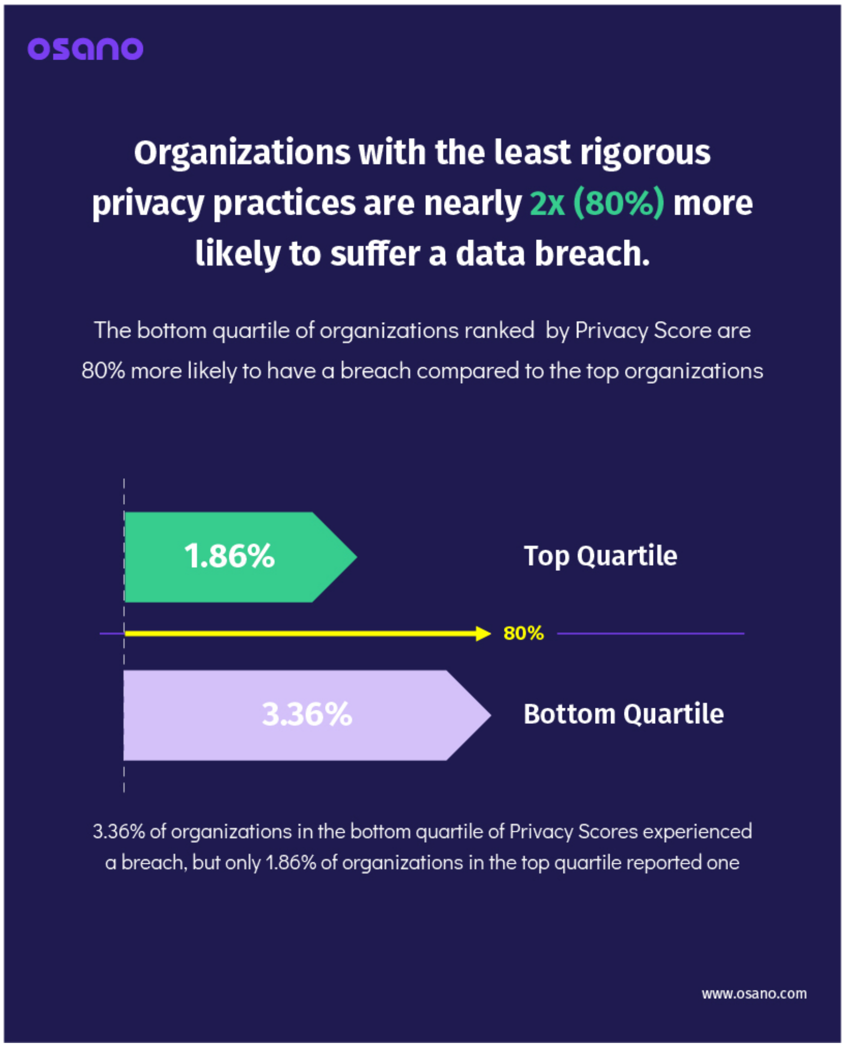
When comparing Privacy Scores for each quartile to profiles of data breaches from the past fifteen years, the results are striking, as demonstrated by the following chart.



If a website ranks in the top 25% of Privacy Scores, their likelihood of experiencing a data breach is approximately 1.86%. For a site in the bottom 25%, though, the probability of facing a data breach is approximately 3.36%.

In other words, websites with the lowest Privacy Scores are nearly twice as likely to suffer a data breach than the top-ranking sites.

Websites with the lowest Privacy Scores are nearly twice as likely to suffer a data breach than the top-ranking sites



Organizations with the least rigorous privacy practices are nearly 2x (80%) more likely to suffer a data breach.

The bottom quartile of organizations ranked by Privacy Score are 80% more likely to have a breach compared to the top organizations

3.36% of organizations in the bottom quartile of Privacy Scores experienced a breach, but only 1.86% of organizations in the top quartile reported one

www.osano.com

Tracking the Data Trail

The correlations between data breaches and Osano Privacy Scores are the result of myriad causes. Websites that willfully ignore or unknowingly overlook best practices increase their exposure to risk. In contrast, businesses that emphasize a culture of responsible data stewardship reduce the likelihood of a data incident.

Among the many reasons for the relationship between data breaches and privacy practices, the research discovered a particularly dangerous source of data breaches: third-party vendors.

Consider the following pieces of information:

- The average company shares its data with 730 different vendors.
- The Internal Auditors Research Foundation found that third-party vendors were responsible for two out of every three data breaches.

Most companies fail to understand the complex ways their data is used by their primary vendors, let alone with the vendors of all of their vendors. When the Department of Justice evaluates whether to file criminal charges against a company, they strongly consider if the company was adequately observing their vendors. There are tools on the market that will monitor vendors, but many businesses do not proactively ensure their clients' information is appropriately safeguarded.

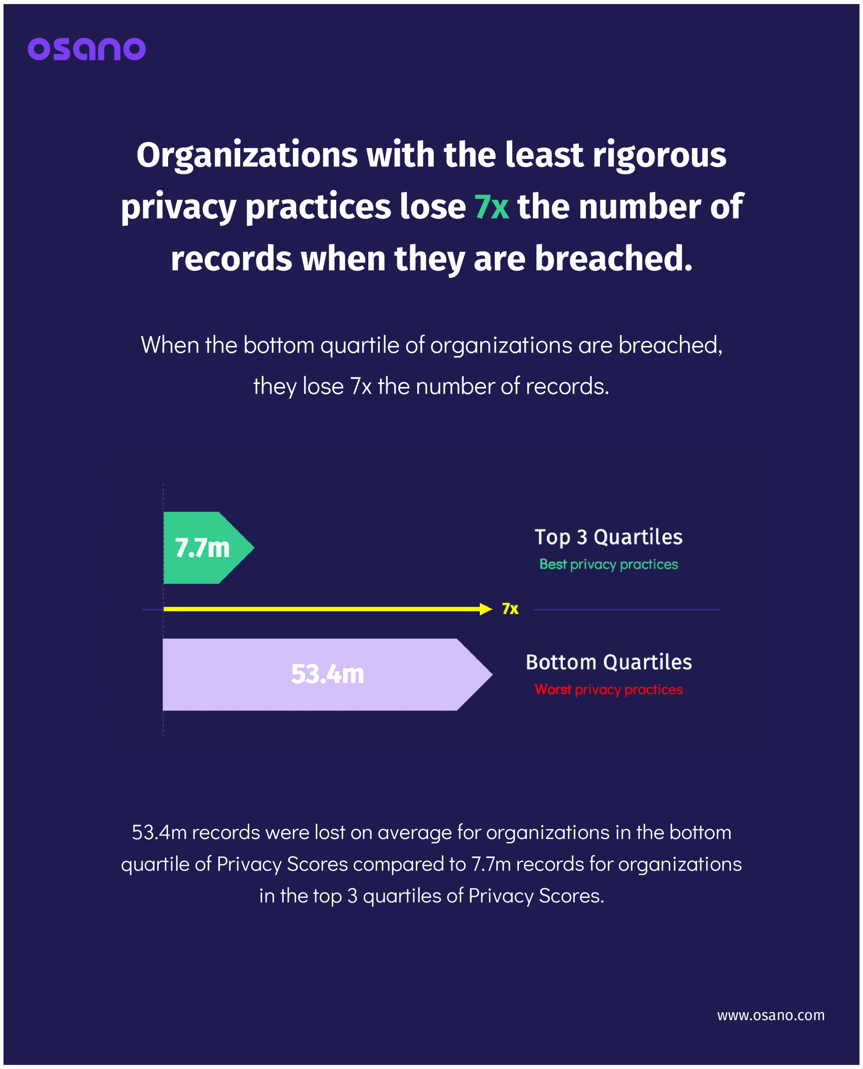
ALL DATA BREACHES ARE NOT CREATED EQUAL

Assessing the Severity of Data Breaches

Do websites with the least rigorous privacy practices suffer from the most damaging data breaches?

Answering this question involved analysis of data from the Privacy Score quartiles. Legislative requirements compel organizations to not only disclose any data breaches but also identify the number of records that were exposed, stolen, or otherwise compromised. In this context, a record typically refers to information for a single person or account. The research confirmed the correlation between organizations' quality of privacy practices and the number of records involved in data breaches.

Companies with the least rigorous privacy practices lose seven times the number of data records when they are breached.



osano

Organizations with the least rigorous privacy practices lose 7x the number of records when they are breached.

When the bottom quartile of organizations are breached, they lose 7x the number of records.

53.4m records were lost on average for organizations in the bottom quartile of Privacy Scores compared to 7.7m records for organizations in the top 3 quartiles of Privacy Scores.

www.osano.com

Organizations in the bottom 25% of Osano Privacy Scores lost, on average, 53.4 million records during a data breach. For organizations that weren't in the bottom quartile of Privacy Scores, each data breach resulted in an average loss of 7.7 million records.

Organizations with the least rigorous privacy practices lost seven times the number of records during each data breach than organizations with the most responsible practices.

Facing the Fallout from Data Breaches

When it comes to millions of lost records, the specific number really matters.

Many privacy laws determine financial penalties for data breaches on a per-record basis. For instance, the California Consumer Privacy Act (CCPA) can impose a fine of $7,500 **per record**. Companies with the lowest Osano Privacy Scores, therefore, face fines seven times larger than companies with the best scores.

Furthermore, data breaches inflict damages far beyond legislative penalties. A recent study identified a negative effect on share prices. For companies trading on the NASDAQ that experienced a data breach, their share price was an average of 13% lower than the Index three years after the incident. In an era of increasing focus on digital privacy, safeguarding a company's data also protects their bottom line.

For companies dealing with the fallout of data breaches, fines and share price are only two of the many possible repercussions. Companies are impacted in many other ways, including the following consequences:

- Reputational damage
- Criminal liability for company executives and board members
- Exposure to class-action lawsuits
- Diversion of company resources and focus toward legal defenses, rather than core activities

Equifax is a canonical example. Their massive 2017 data breach resulted in a $700 million fine from the Federal Trade Commission. The impact on their reputation, though, will be difficult to measure and take a long time to repair. As a result of that breach, the company's name became synonymous with irresponsible data management.

ADDITIONAL FINDINGS

Identifying the Causes of Data Breaches

Establishing best practices for data privacy requires a clearer determination of whether most data breaches are caused by careless mistakes, nefarious attacks, or unknown issues.

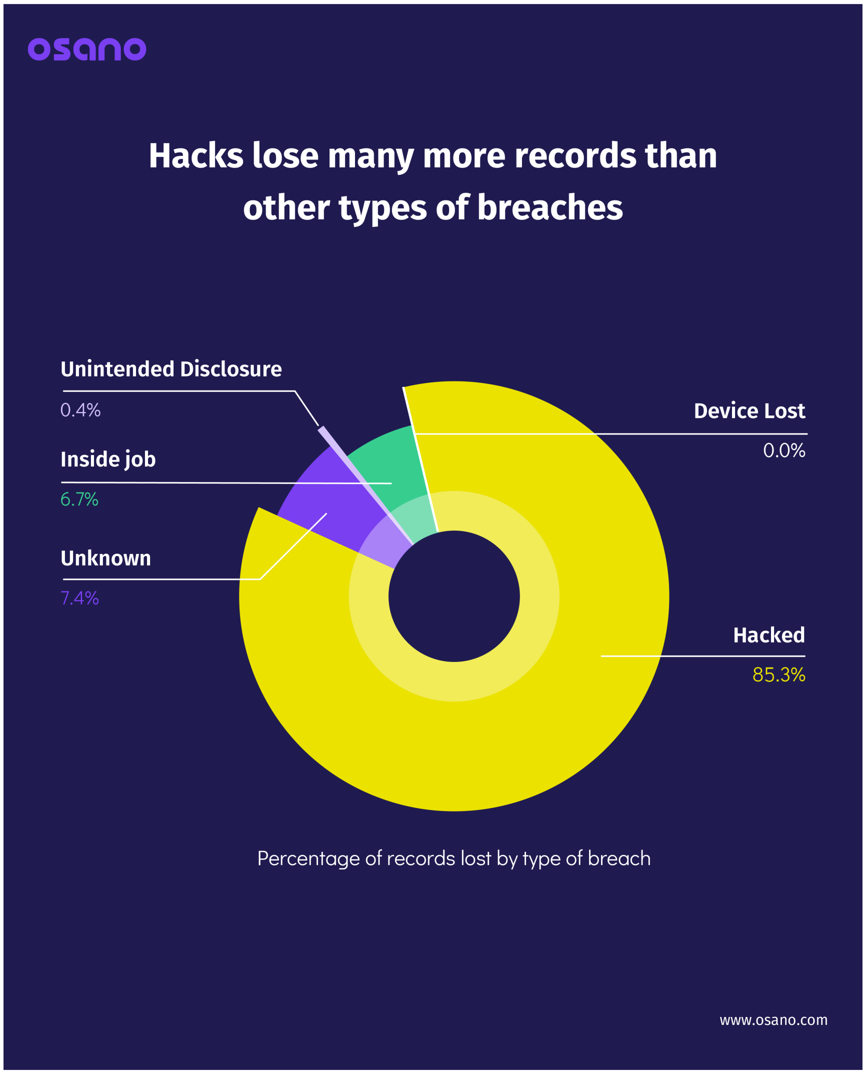
The analysis of previous data breaches identified a number of causes:

- **Unintended internet disclosure** — Personal information was left unencrypted on a publicly accessible website or computer.
- **Unintended physical disclosure** — Credit cards, computer devices, and paper documents that contained personal information were stored improperly or lost.
- **Inside jobs** — Access to personal information was granted by the deliberate assistance of an employee, contractor, or other party.
- **Hack** — Personal information was accessed by hackers who intentionally attacked a system for illegitimate purposes.
- **Unknown** — Any disclosures where the source of the data breach could not be verified.

Conventional wisdom among privacy professionals suggests that most data breaches fall within the category of unintended internet disclosure. This new research contradicts that perception.

Hacker attacks were responsible for the highest number of data breaches. Plus, hacker-caused data breaches inflicted the most severe losses. On average, hacker attacks exposed 17 times more records than other breach types.

Hacker attacks were responsible for the highest number of data breaches and inflicted the most severe losses.

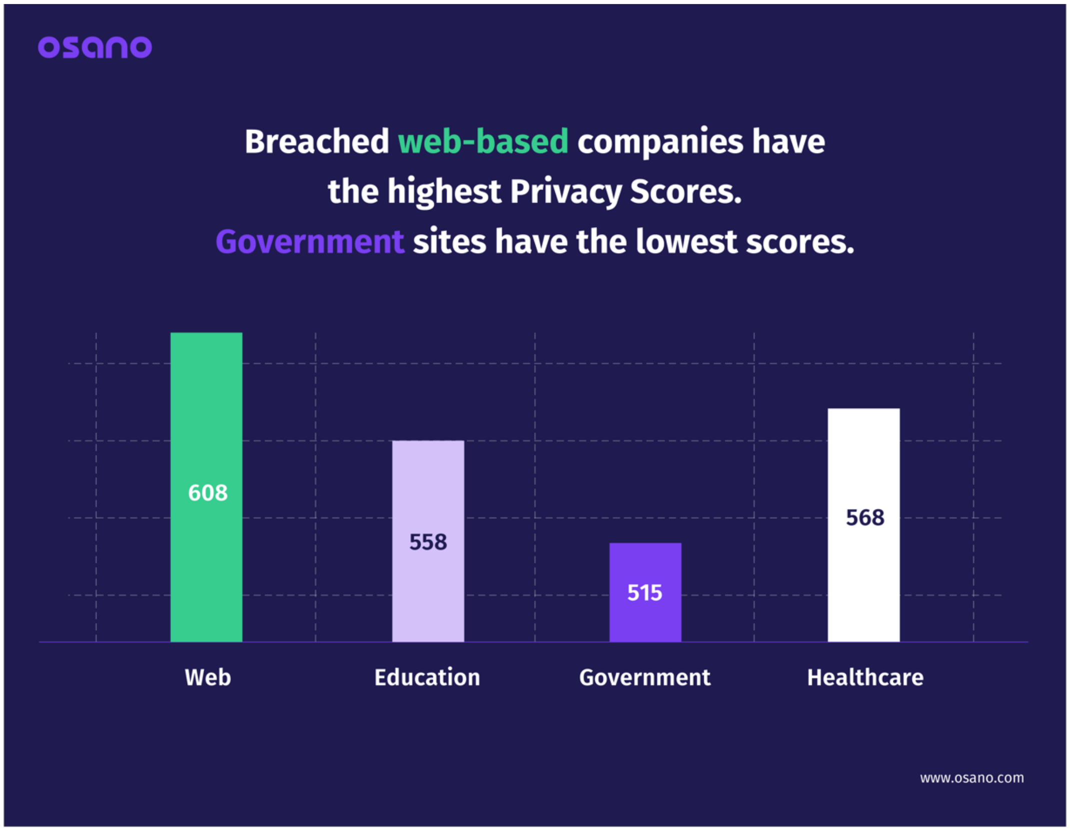


The Unknown category presents an additional set of challenges. Without clear information about the source of the data breach, organizations are unable to diagnose which part of their data security system failed. As such, businesses cannot rectify their problems and bolster their privacy plans. The research noted that websites with the lowest quartile of Osano Privacy Scores were more likely to report the source of a data breach as Unknown.

One additional caveat: businesses interested in privacy cannot overlook the prevalence of unreported data breaches. Whether to avoid legislative fines or reputational ruin, some organizations willfully avoid disclosing information about data breaches. The information on this topic is sparse, but some analysts estimate that more than half of all data breaches go unreported. Osano supports regulatory measures that improve internet transparency and reinforce people's right to privacy.

Examining Industry Trends

Analysis of data practices by industry type confirms that some industries manage data privacy better than others. Web-based companies generally earned higher ratings for their practices. On average, government websites received lower Osano Privacy Scores than private corporations.



Among all entities, **companies in financial industries were far more likely to experience data breaches caused by inside jobs**. Companies in financial industries represented 14% of the profiles in our dataset, yet they were associated with 45% of all inside job data breaches — three times the frequency you would expect.

Examining Top-Level Domains

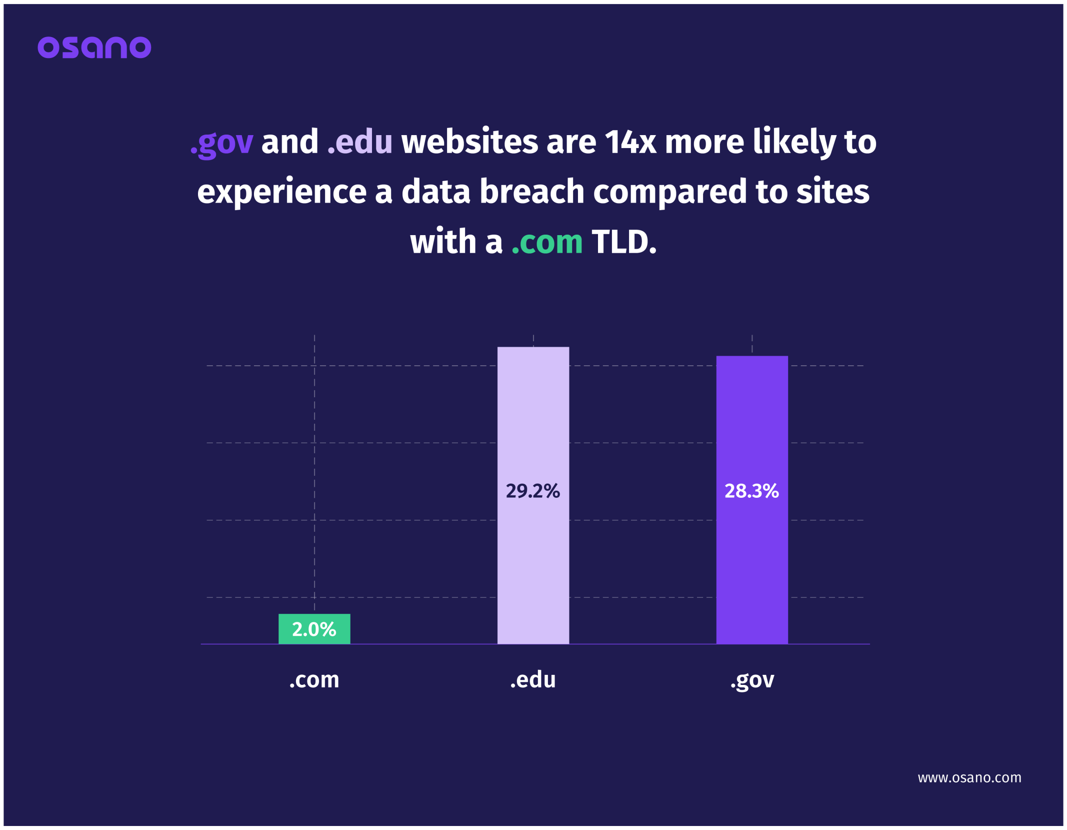
Nearly 30% of government and educational organizations with “.gov” and “.edu” top-level domains experienced a data breach.

Osano’s team also analyzed the results by top-level domains (TLDs), the last component of a website address, such as “.com.”

In our dataset, approximately two-thirds of the websites used a “.com” TLD. Other common TLDs included “.edu” and “.gov.”

By examining the TLD of each data breach, Osano observed the following information:

- Organizations with “.com” TLDs earned, on average, higher Osano Privacy Scores than those using other TLDs.
- An astonishing 30% of organizations with “.gov” and “.edu” TLDs experienced a data breach — more than 14 times the rate of “.com” TLDs.


.gov and .edu websites are 14x more likely to experience a data breach compared to sites with a .com TLD.

- Among the government websites scored, federal agencies earned higher Privacy Scores (595) than state-level websites

(541). The relationship between data breaches and Privacy Scores again holds true in this case. Sixty-three percent of state government sites have been breached, compared to 11% of federal agency sites.

Data privacy is a continual process, not a definitive accomplishment. Osano continues to update our dataset and investigate trends so that companies can spend less time focused on privacy and more time on what they do best.

YOUR FUTURE AS A PRIVACY-MINDED ORGANIZATION

What does the future hold, in terms of data privacy?

After a thorough examination of the privacy practices from more than 11,000 companies and organizations, Osano identified three key trends for 2020:

- Increasing complexity of vendor policy changes and notifications
- Growing public concern about data privacy
- Expanding legislative activity addressing data security

Trend 1: Increasing Complexity of Vendor Policy Changes and Notifications

As the corporate world continues to embrace software solutions, there has been a fundamental shift in the nature of policy agreements. Instead of standalone contracts, users now enter into self-updating terms and conditions that change with remarkable frequency. Many vendors actually revise their policies once a month. Even more alarmingly, fewer than 25% of vendors send notices that communicate changes to privacy policies.

As noted earlier in this report, the average company shares its data with 730 different vendors, and third-party vendors were responsible for two out of every three data breaches. In this atmosphere, manually reviewing changes to policy notices is untenable. **Websites require automated solutions that monitor updates and flag concerns.**

Trend 2: Growing Public Concern About Data Privacy

Consumers are learning more about corporate privacy practices, and they are voicing their concerns. According to a 2020 study from Pew Research Center, **more than half of all American adults stated they decided against using a product or service due to privacy concerns**.

Events like the Facebook and Cambridge Analytica scandal prompted people to reexamine their relationship with social media platforms. Pew Research Center has found that two-thirds of adults believe that the risks of data collection outweigh the benefits.

Trend 3: Expanding Legislative Activity Addressing Data Security

Significant legislative activity around data privacy and security is expected in the coming years. Despite polarizing views on many political issues, Americans are unified in their concern about data privacy. To that end, 72% of U.S. adults support a national privacy law.

In 2018, the European Union implemented the General Data Protection Regulation (GDPR) — the most far-reaching data privacy legalization passed by any government. In the United States, California led the way with the California Consumer Privacy Act (CCPA) signed into law on June 28, 2018.

Nevada imposed a more modest set of regulations in November 2019. Maine’s Act to Protect the Privacy of Online Consumer Information took hold on July 1, 2020, and at least nine more U.S. states are currently pursuing data privacy laws.

Even though many countries and U.S. states have yet to implement their own regulations, companies should note the global reach of privacy legislation — the GDPR protects E.U. residents even when they visit American websites.

Moving from Reactive to Proactive

As we’ve all learned in 2020, companies cannot anticipate and prepare for every possible crisis.

All organizations remain vulnerable to damaging data breaches, especially due to the increasing sophistication of hackers. By prioritizing a review of privacy and security practices, organizations can demonstrate their trustworthiness to investors, clients, and customers.

If an organization is concerned about their website’s privacy practices, here are some concrete steps they can take to reduce their exposure to risk:

1. **Consent Management**
   Ensure that visitors to all websites are presented with a clear choice to opt in (or out) of cookies, scripts, tracking, and third-party data sharing. All consent messages must be customized for the privacy laws of each visitor’s jurisdictions and displayed in their preferred language.
2. **Data Subject Rights**
   Put a system in place to comply with the many laws granting individuals the right to delete, modify, or request the personal data that the organization holds.
3. **Data Mapping**
   Complete a data-mapping exercise to understand how and where the system stores and moves data.
4. **Vendor Monitoring**
   Continuously monitor how the data is shared — not only with primary vendors but also with third-party vendors down the line. Track updates to privacy policies, identify risky vendors, and develop an ecosystem of partners that share organizational values.

If you are unsure about where you currently stand or how to get started, we recommend you conduct a free privacy audit of your website. If you are ready to speak to someone about improving your organization’s privacy, the team at Osano is here to help.

ABOUT OSANO

Osano is an easy-to-use, complete data privacy platform that quickly helps businesses comply with virtually all privacy legislation around the globe. Platform features include consent management, data subject access requests, GDPR representative services, and vendor monitoring.

Osano’s cookie consent management software is the most widely used in the world. More than 750,000 organizations trust Osano to ensure more than 2.5 billion monthly visitors comply with data privacy legislation.