Data Privacy in California: An In-House Counsel's Roadmap for Protecting Against Increasing Threats

Cybersecurity threats aren't new, but the risks and compliance challenges are growing — particularly for businesses operating in California. After successfully targeting larger global corporations, who have now beefed up protections in response, many cybercriminals have shifted their focus to smaller companies that may not have security entirely buttoned up.

While small and midsize businesses may not house vast amounts of data on the same scale as multinational corporations, they often lack the resources to effectively guard against cyberattacks, making them attractive targets. Consumers are also more aware of data privacy risks and expect stronger protection from the companies they engage with regardless of their size. Failing to meet these expectations can mean more than reputational damage; it can result in costly regulatory penalties and liabilities.

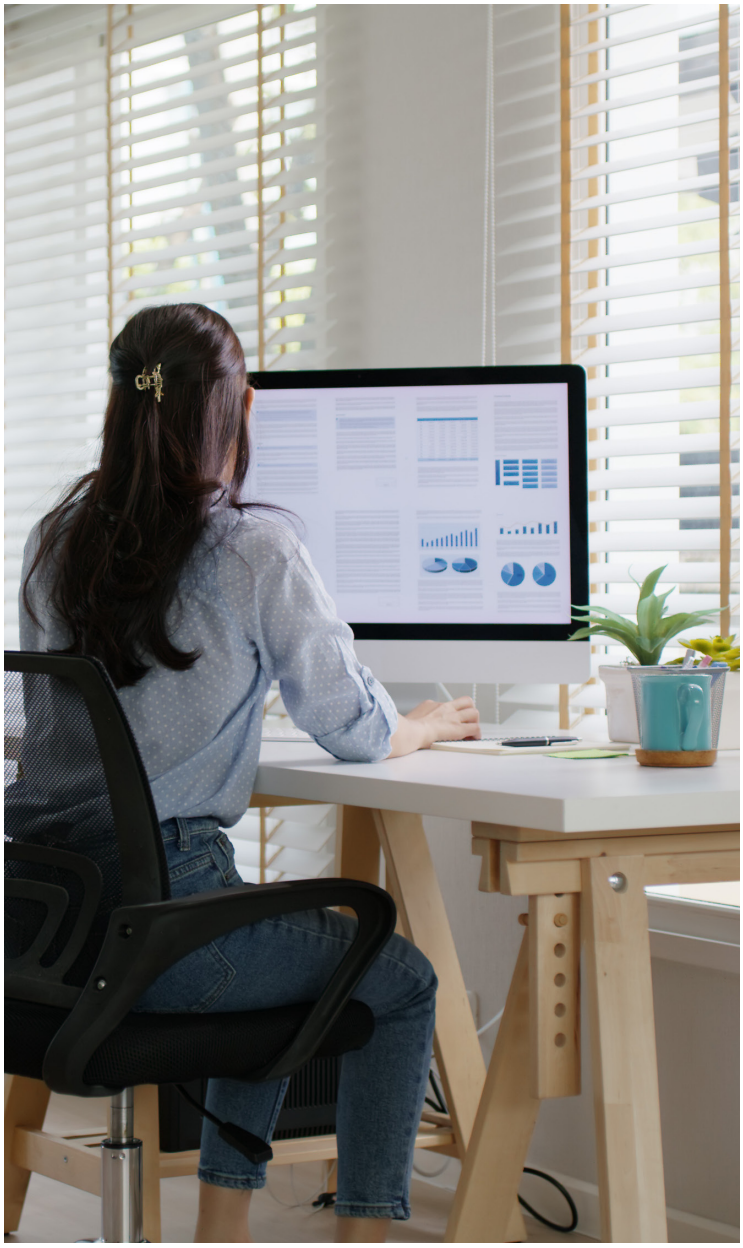
The global average cost of a single data breach is now $4.88 million, which is a 10% increase from the prior year and the highest-ever total, according to a report by IBM and the Ponemon Institute. Nearly half of all 2024 breaches involved customer personal data, while one in three went after shadow data — meaning it was stored outside a company's IT security measures or data management system.

For in-house counsel, this means taking the lead on your company's data privacy strategy. A robust plan should be proactive, tailored to your company's specific risks, and focused on both compliance and security. Here's what you need to know and do to protect your company.

1 Understand your company's unique risks

First, understand that no company is too small to target. Some small businesses may underestimate the risk of cyberattacks because of their size, leading to complacency in security practices. Don't let that be you. It's important to know where risk lurks to implement protections, and some of these vulnerabilities are unique to small companies.

- **Reliance on digital platforms**: Small and midsize businesses are relying on more digital tools for operations, marketing, and sales to streamline efficiency and reach wider audiences. But this reliance also exposes sensitive customer data and business operations to breaches and other cyber risks.
- **Limited cybersecurity resources**: Without dedicated cybersecurity teams, many businesses lack sufficient expertise to prevent or respond to threats. This creates vulnerabilities that bad actors can exploit.
- **Remote work**: Remote and hybrid work arrangements have expanded the attack surface, with unsecured home networks and personal devices becoming potential vulnerabilities. Likewise, increased reliance on mobile devices for work opens new attack vectors. Employees accessing company systems from unsecured devices or networks can unintentionally create entry points for cybercriminals.
- **Regulatory compliance challenges**: As a leader in consumer protection, California's data privacy laws (including the California Consumer Privacy Act, or CCPA) set some of the highest standards in the country. While these laws are a positive thing for you and your customers, they can pose significant compliance challenges for businesses that don't have the expertise or resources to meet regulatory requirements.



CEB

2 Assess the security of the data you're storing

While the details will vary by industry, California law typically requires data security measures to be reasonable, appropriate, and adequate.

Start by identifying the types of sensitive information your company collects and stores, such as employee records, customer data, financial details, intellectual property, or health information. Next, list all the locations where this data is stored or transmitted, including cloud systems, company networks, external drives, employee devices, and third-party platforms. Don't overlook remote work, as personal devices and unsecured networks often introduce risks.

Once your inventory is mapped out, conduct an audit to assess vulnerabilities. The following questions can help you uncover weak points and ensure your data is secure:

- **How is the data acquired or created?** Identify how sensitive information enters your company's possession and whether those processes introduce unnecessary risks.
- **Where is the data stored?** Assess whether storage systems — including physical archives — are secure, encrypted, and compliant with relevant regulations.
- **How is the data protected?** Evaluate whether safeguards, such as access controls, encryption, and monitoring tools, are in place and effective.
- **How is the data shared, transmitted, or deleted?** Ensure proper protocols exist for securely sharing data with third parties, removing sensitive information from unauthorized devices, and adhering to your company's document retention and destruction policies.

For each vulnerability you identify, assess:

1. How likely is the threat to occur?
2. What would the consequences be if it happens?
3. Are current policies and safeguards sufficient to minimize this threat?

CEB

3 Build your data security plan

For smaller companies with limited resources, a focused and practical plan can make all the difference in preventing breaches, protecting customer trust, and maintaining compliance with California's rigorous data privacy laws. This is where it's crucial to factor in the specific risks and operational realities of your business that you identified above.

Here's how to get started:

- **Keep it clear and relevant**: Draft policies in plain, straightforward language to ensure everyone in the organization, regardless of technical expertise, can understand and follow them. Align these policies with your company's overall goals and operations to avoid confusion or conflicts. Employees should be made aware that these policies are non-negotiable, so include details about the consequences of noncompliance, whether it's related to ignoring security protocols or mishandling sensitive data.
- **Tailor measures to your risks**: Address the specific risks your company faces by considering the type of data you handle, the threats you've identified, and the likelihood of an incident occurring. If your company processes sensitive financial data, For example, if your company processes sensitive financial data, this might mean implementing robust encryption and monitoring systems. When managing proprietary information, focus on access controls and insider threat prevention. Your safeguards should be proportionate to the value of the data you're protecting and the potential impact of a breach.
- **Identify which regulations apply**: Determine which laws, regulations and industry standards your company needs to comply with. For instance, if you handle consumer data, the CCPA likely applies. The Health Insurance Portability and Accountability Act (HIPAA) will be relevant if you work with health-related data. If your business operates in multiple jurisdictions, you should also consider international regulations such as the General Data Protection Regulation (GDPR), which applies to the data of all EU residents. CEB's cybersecurity explainer includes a detailed chart connecting specific security measures with their corresponding laws, regulations, and guidance.
- **Don't forget about physical IT assets**: Protecting data stored in a physical place is just as important as securing digital systems. This includes restricting access to servers, workstations, and storage devices, especially for smaller companies that may have fewer layers of physical security. You should also establish controls for the safe removal or disposal of old hardware and storage devices.
- **Prepare for dual threats**: While your data security plan will focus on digital risks, consider integrating it into a broader emergency response strategy. Your protocols for any unexpected challenge should seamlessly cover cybersecurity breaches and physical threats such as fires or earthquakes. This ensures a cohesive and efficient approach.
- **Establish a plan for disclosing breaches**: California's security breach disclosure law under Civil Code section 1798.82 requires businesses with personal information about California residents to inform them if someone without permission may have accessed their unencrypted personal information. Establish notification procedures for affected individuals, regulators, and possibly even the media.
- **Create a backup and recovery plan**: Regularly back up critical data and store it securely in a separate location, such as a cloud-based service or an offsite facility. Establish clear procedures for restoring lost or compromised data and test the recovery process periodically to ensure it works. This will help minimize downtime and reduce the impact of a security incident.

Be sure to incorporate the cybersecurity plan into your employee handbook and require all relevant employees to review and acknowledge it in writing. This not only reinforces the importance of compliance but also ensures that everyone understands their role in safeguarding company data.

CEB

4 Review all third-party vendors' security measures

If only it were enough to have your own house in order when it comes to data security, but alas, third-party relationships bring their own risks. Every vendor you rely on can become a potential entry point for cyber threats, making it essential for you to rigorously evaluate their security practices as in-house counsel. As smaller businesses are often reliant on external providers for IT, payment processing, and cloud services, you will likely face heightened vulnerabilities if your partners fall short on cybersecurity measures.

Before entering into agreements, assess whether the vendor can adequately protect your company's data and meet legal and regulatory obligations. To safeguard your organization, consider including the following provisions in your vendor contracts:

- **Require robust data security safeguards**: Vendors should implement measures that appropriately protect the confidentiality, integrity, and availability of the data they handle on your company's behalf.
- **Restrict subcontracting**: Prohibit or strictly control the use of subcontractors to prevent risks from cascading to unknown entities.
- **Mandate incident reporting**: Require vendors to notify you promptly of any security incidents and specify how they will address breaches, including disciplining or terminating personnel responsible.
- **Allow audits**: Ensure your company has the right to audit the vendor's policies, procedures, and contract-required documentation to verify compliance.
- **Include termination clauses**: Grant your company the ability to terminate the contract if the vendor breaches a material term, particularly those related to data security.

5 Educate your team

Your attorneys and staff are the first line of defense against cyber threats, so they must understand how to identify and avoid risks. Small and midsize companies are frequently targeted by phishing and business email compromise schemes due to less robust employee training and awareness programs compared to larger organizations.

Regularly communicate security policies, updates, and best practices through ongoing training sessions and easy-to-follow guidelines. Provide written copies of policies, require employees to acknowledge receipt, and conduct mandatory training on common issues like phishing and social engineering.

While security breaches may require disciplinary action, consider offering an anonymous reporting system to encourage staff to share concerns without fear of retaliation.

6 Stay ahead of changing regulations

Data privacy regulations are constantly evolving, not only at the state level but also nationally and internationally. The GDPR has set the standard for data protection globally, but understanding all regulations will help prevent your company from facing significant legal issues as international privacy laws become more stringent.

CEB's data privacy content can help you digest and plan for the key requirements, while Daily*News* coverage can keep you up to date on the latest developments.

Assume a breach is coming

As much as we wish them away, data breaches can still occur despite our best efforts — and smaller companies are uniquely vulnerable. The best way to prepare is to assume a data breach is going to happen and put a plan in place for it.

As a trusted advisor to your company, it's your responsibility to advocate for and help develop a data privacy strategy that minimizes risk and helps build and maintain trust with your customers and partners. With the right legal, technical, and operational safeguards in place, you can protect both your company's reputation and its bottom line in an increasingly data-driven world.

Add CEB to your strategic toolbox by scheduling a demo — and check out these frequently asked questions.

CEB

Contact us at 1-800-232-3444 or visit us online to learn more.