



5 data privacy and cybersecurity tips for construction firms

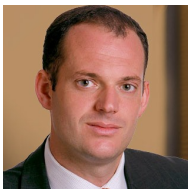
OWEN QUINN, HUSSEIN JAWARD, CIPP/US | DATA PRIVACY SOLUTIONS | SEP 12, 2019

No industry is immune from data privacy and cybersecurity threats, [and that includes the construction industry](#). Here are five data privacy and cybersecurity tips construction firms should consider putting to use to protect themselves against these looming threats.

1. **Minimize the amount of data your organization retains.** The best way to protect any organization from data security threats is to retain as little data as possible. For example, a construction firm may need to collect prospective employees' Social Security numbers as part of the hiring process. But how long does it really need to hold on to that information? Certainly not indefinitely. Rather, a construction firm should dispose of any and all sensitive data that is non-essential to its business operations as soon as it is able to. Doing so reduces the likelihood the data will be breached at a later date.
2. **Protect your organization with the right data privacy contractual provisions.** Data privacy laws only impose baseline requirements. For example, state data breach notification laws may require a contractor that maintains a subcontractor's employees' personal information to notify the subcontractor when that information is breached. But the subcontractor can also bargain for more protections at the time it is engaged by the contractor. For instance, the subcontractor can insist the contractor agree to indemnify it for any claims lodged against it for the contractor's mishandling of personal information.
3. **Designate a privacy officer.** New threats to data privacy and cybersecurity emerge every day. Construction firms should make at least one employee responsible for keeping the organization informed of such threats, promulgating data security best practices, and training employees on such issues.
4. **Engage information technology and forensic experts—and data privacy and cybersecurity attorneys—to help you determine your organization's privacy vulnerabilities.** Data privacy and cybersecurity risks are not always apparent to laypersons. Engaging information technology and forensic experts can help organizations identify and remediate those risks. And having an attorney present in discussions with such experts can cloak communications with the attorney-client privilege—and thereby prevent an expert's findings from being used against a construction firm in subsequent data privacy and cybersecurity litigation.
5. **Invest in a cyber-liability insurance policy.** IBM estimates that as of 2019, the average cost of a data breach is \$3.92 Million. Investing in a cyber-liability insurance policy can defray some or all of the costs associated with a data breach.

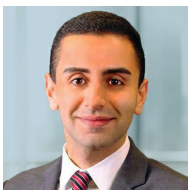
Construction firms face numerous data privacy and cybersecurity risks every day. These tips are simple and easy ways to begin to mitigate those risks.

Attorneys from McDonald Hopkins' Construction Practice Group and Data Privacy and Cybersecurity Practice Group are available to assist construction firms address current and emerging data privacy and cybersecurity vulnerabilities, achieve compliance with data privacy law before and after data security incidents, and litigate data privacy and cybersecurity disputes.



OWEN QUINN

[Read More](#)



HUSSEIN JAWARD, CIPP/US

[Read More](#)