Professional Warranty Service
PWSC CORPORATION

Home Building & Data Security: What Can Builders Do to Help Protect Their Clients

Target made national headlines five years ago when hackers exposed the debit and credit card information of more than 41 million customers. The widely publicized data breach cost the retail chain $18.5 million in a multi-state settlement—the largest data security payout in the history of cyber crime up to that point.

What many people don't know, however, is that the data breach occurred because hackers stole the login credentials to the retailer's payment system from an unprotected HVAC contractor.

Since then, the stakes have only gotten higher as a growing number of high-profile companies grapple with the financial fallout and devastating reputation loss that can accompany data security failures. Sometimes the company is at fault, like when Wells Fargo got fined $185 million for creating unauthorized bank and credit card accounts on behalf of unsuspecting customers. Sometimes it's the result of questionable data security practices, such as when Cambridge Analytical harvested the personal data of 78 million Facebook users, resulting in one of the largest data breaches of all time.

For home builders, however, cyber crime might seem like a distant threat. After all, construction hasn't traditionally been a high-tech field. A construction company—even a large one—isn't as lucrative a target as, say, a financial services firm. And most home builders are small to midsize companies that surely aren't even on the radar for hackers, who are more likely to pursue bigger fish.

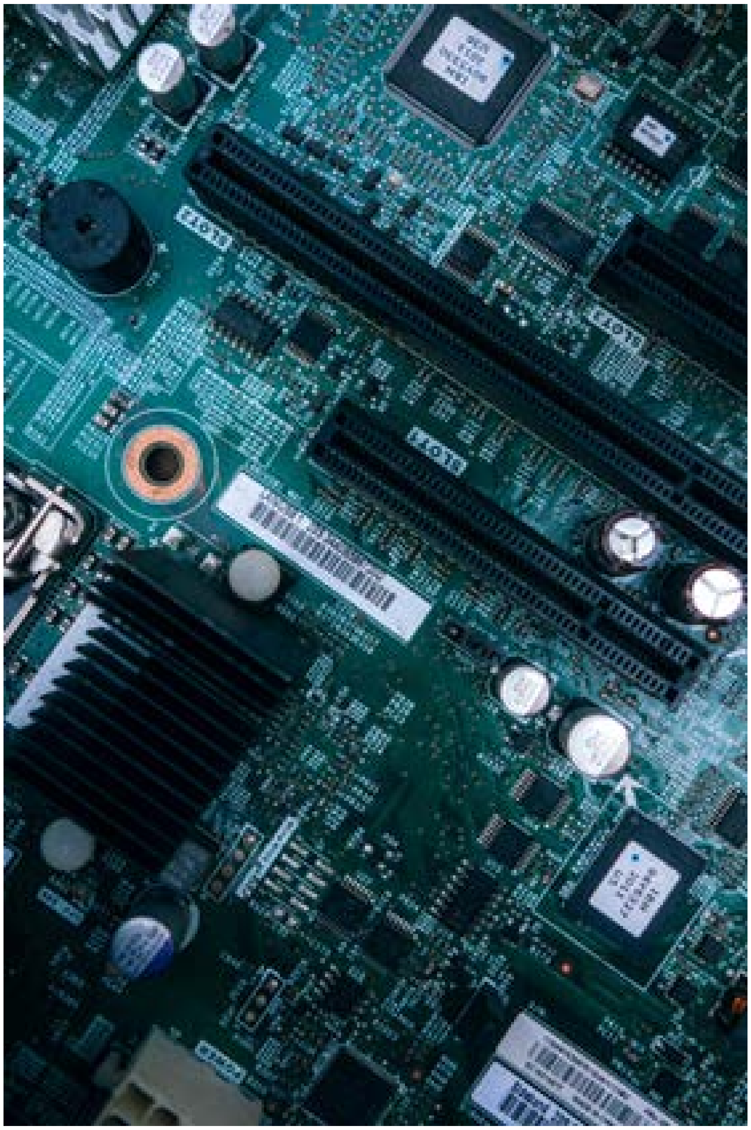
But this is exactly the type of thinking that makes smaller construction firms prime targets for cyber criminals, "because many don't believe it will happen to them," says Todd O'Boyle, chief technology officer for Percipient Networks.

It can and does happen. A recent Forrester survey found that more than three in four respondents in the construction, engineering and infrastructure industries had experienced a cyber security incident within the past year. Even small builders have access to a wealth of valuable information hackers would love to get their hands on, from employee payroll data to architectural drawings and other proprietary assets. And in a potentially lucrative field with high cash flow, a builder's vendors can represent an especially alluring prize for hackers, who may target general contractors or subcontractors in an effort to access their clients' networks—just like they did with Target's HVAC subcontractor.

Cyber security isn't just for tech companies or financial giants. It's an essential part of any home builder risk management strategy. And given how crucial referrals are for any home builder, reputation management experts in the field also need to make data security a priority.

> "With nearly every aspect of the home building industry moving online and most information stored in digital formats, it's time for every home builder to seriously assess their cyber security and potential exposure to liability," says the National Association of Home Builders.

"Loss of trade secrets, loss of reputation and even illicit bank account access are certainly huge concerns in a cyber attack. But the liability associated with exposing others' personal and sensitive information to intrusions is where the real risk lies," says the NAHB.



Why home builders are at risk of a data breach

If home builders lag behind in implementing sound data security practices, it's largely due to the fact that the construction industry has been notoriously reluctant to embrace new technology. But as more firms adopt internet-connected solutions such as Building Information Modeling, Integrated Project Delivery and file sharing, the risk of a potential data breach is growing.

It doesn't take a lot of fancy software to make a company vulnerable to hackers. All it takes is one employee with an email account—as Turner Construction, one of the largest U.S. construction management firms, discovered in 2015 when an employee fell prey to a phishing scam and mistakenly forwarded employee earnings and tax information to a fraudulent email address. All it takes is a single subcontractor with lax security practices, as Target found out in 2013.

How to minimize subcontractor security risks

Every company needs basic data security measures to protect their employee information, customer data and proprietary information. But home builders also have unique vulnerabilities that put them at particular risk, including their heavy reliance on subcontractors. Two in three builders say they subcontract out as much as 75 percent of their total construction costs for work on a typical single-family house, employing an average of 22 subcontractors in the process. Because these subcontractors are often privy to proprietary and client information, each one represents a potential weak link in the data security chain.

> "As third-party vendors to clients, who also use third party suppliers and subcontractors themselves, construction companies are exposed to stakeholder breach liability risk on all sides," says Risk & Insurance contributor Allied World.

The problem with subcontractors is that builders often don't have any insight into or control over their data security practices—yet if a breach occurs, the builder could still be held liable. According to the National Labor Relations Board, subcontractors can in some cases be considered "joint employees" of their employers, which can have serious implications for builders when it comes to cyber security. That's why creating a firm data security policy and ensuring subcontractors comply with it is an important first step in home builder risk management.

When home builders fail to address these issues, it's not because they're being intentionally neglectful. Most are simply focused on doing what they do best, which is completing construction projects on time and on budget.

Data security is a moving target at best, as hackers continually find new ways to get around common security measures, and managing these risks in-house demands a significant time investment. Many builders simply don't have the time or expertise to keep up with the latest security developments.

To free up time for builders to evaluate data security risks, a partner such as PWSC can help guide builders in other risk management areas, such as:

- Choosing and maintaining the right risk transfer instruments, from insurance policies to structural home warranties.
- Setting appropriate homeowner expectations regarding home maintenance, and warranty requests and issues.
- Specifying clear processes and procedures should a dispute occur as well as providing proven mediation and arbitration methodologies to avoid litigation

In addition to administering builder home warranties, PWSC's highly experienced team proactively monitors regulations, new legislation and other developments to remain apprised of changes in the construction risk landscape. Our vigilance and home builder legal expertise helps builders manage and limit liability risk exposures with confidence.

Professional Warranty Service
PWSC
CORPORATION
Confidence You Can Build On.

This report is a product of PWSC, an indispensable risk management partner in the new home construction ecosystem with a relentless focus on integrity, innovation, and customer service. They are experts when it comes to mitigating risk, home builder warranties and warranty solutions, and home warranties for home buyers. We invite you to learn more about PWSC.

Professional Warranty Service Corporation (PWSC) headquartered in Chantilly, Virginia, provides innovative risk management solutions to promote homeownership to the largest tier of domestic residential construction firms.