How to Build a Human Firewall from the Ground Up

By Patti Walsh

As the residential construction industry continues to realize—and leverage—the benefits of digital technology, the conversation surrounding such technologies is shifting. Suddenly, builders, developers and contractors are no longer asking whether it makes sense to invest in the cloud, mobile devices or the latest building information modelling software. Rather, they're looking for ways to remain technologically relevant while simultaneously keeping their businesses safe.

This is no easy task. As the cyber landscape rapidly evolves from one day to the next, it's clear that a standard anti-virus program isn't going to cut it. But with limited resources at hand—particularly in the areas of IT staff and budgets—building and managing a robust cybersecurity program seems unattainable particularly for smaller residential construction businesses.

Fortunately, there are countless things you can do to defend your business on a small cyber budget—the most effective being building a cyber-aware workforce.

A Threatening Place

While IT security systems offer a valuable layer of cyber protection, the truth is half of all cyber breaches start by targeting organizations' email systems and browsers. If that number seems high, keep in mind that today's hackers are significantly more advanced than those of the past—and, as such, cyber attacks are much more difficult for an untrained eye to identify.

To give you an example of what a cyber breach may look like, imagine your company possesses valuable information that competitors would love to get their hands on. A savvy hacker, recognizing this, sets out to steal it with the intent of selling it to your competitors. To do this, he first needs to find employees with access to the company's data and systems—so he scours social networks until he finds one, making note of any colleagues on the individual's friends list.

Next, the hacker creates a fake but recognizable email address—maybe ending in .ca instead of .com—to impersonate the targeted invidual's colleagues or boss, and sends a personalized email with a link. Once the link or attachment is clicked, the hacker is able to install malware—either into the company computer system, the individual's computer or a mobile device—giving the hacker backdoor entry into the company's systems, where he can easily steal the desired information.

First steps: Building a human firewall

While building a human firewall may seem like a huge task, there are three simple things your company can do right now to set you well on your way.

- Strengthen your passwords. Put rules in place to make sure passwords are strong and changed regularly.
- Limit data access. Make sure only those that "need to know" have access to sensitive data.
- Put cybersecurity processes in place. Whether someone loses a mobile device or receives a suspicious email, they should know who to call—and what the process entails.

Elements of a Human Firewall

The key to preventing breaches like these lies in increasing the awareness of employees and end users to such a level that they become a line of defence in their own right—in essence, a human firewall. Just as insulation inside a home's walls is needed to keep cold air out, a human firewall is essential to keep malicious hackers at bay. A sound cyber awareness program consists of three integral components: education, testing and governance.

The first component, education, refers to cyber awareness training offered during the onboarding process and to existing employees. Because cyber threats are constantly changing, employee training should be an ongoing process, not a one-time event. Think of it as a plan toward building a human firewall. When you're building a house, you don't look at a set of blueprints once—you review them regularly, making sure everything is built to spec as you go along. Cyber awareness training should be approached in a similar manner.

Just as cyber awareness training should be ongoing, so should your organization's efforts to test employee and contractor cyber knowledge. To ensure your training program is effective, it's important to define the metrics you want to track and measure ahead of time—and periodically test your people's awareness in various ways to make sure those metrics are improving. To get the most out of the tests, try to make them real for your employees—for example, go undercover and create mock emails from the site superintendent asking them to click on a link.

The third element of a human firewall is strong governance. Through automated reporting and analytics, you should be able to track your cyber awareness progress over time and determine the effectiveness of your awareness training.

A strong cyber-awareness training program should

- Introduce best practice policies to build awareness;
- Be interesting, personal and real;
- Be part of everyday behaviour;
- Make it easy for people to report suspicious emails, a potential cyber attack or other concerning behaviour; and
- Clearly outline your company's cybersecurity processes.

Ahead of the Game

Given the interconnected nature of the construction industry, and the growing prevalence of cyber threats, a human firewall isn't just nice to have—it will likely be a mandatory cybersecurity measure for any business hoping to land major construction projects in the future. With that in mind, early adopters that invest in cyber awareness programs now—and demand the same from their suppliers and contractors—will inevitably be ahead of the curve when that time comes. Those that don't, however, may find themselves falling behind and potentially exposing themselves to a higher risk of a cyber attack—and the financial and reputational loss that often comes along with it.

Patti Walsh is a partner with Grant Thornton LLP in Edmonton. She works with organizations of all sizes in the construction and real estate sector. Patti can be reached at Patti.Walsh@ca.gt.com or by phone at 780-401-8246.